Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Payments and banking with mobile personal devices

Full text Html (32 KB), Pdf (153 KB)

Source **Communications of the ACM** archive
Volume 46 , Issue 5 (May 2003) table of contents
Wireless networking security
Pages: 53 - 58
Year of Publication: 2003
ISSN:0001-0782

Author Amir Herzberg Bar-Ilan University, Ramat Gan, Israel

Publisher ACM Press New York, NY, USA

Additional Information: abstract references index terms review collaborative colleagues peer to peer

Tools and Actions: Discussions Find similar Articles Review this Article
Save this Article to a Binder Display in BibTex Format

DOI Bookmark: Use this link to bookmark this Article: http://doi.acm.org/10.1145/769800.769801
What is a DOI?

ABSTRACT

Mobile devices enable secure, convenient authorization of e-banking, retail payment, brokerage, and other types of transactions.

REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 Bellare, M., Garay, J., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Van Herrenweghen, E., and Waidner, M. Design, implementation, and deployment of the iKP Secure Electronic Payment System. J. Select. Areas Commun. 18, 4 (Apr. 2000), 611--627.

2 Herzberg, A. Micropayments. In Advances in Payment Technology for E-commerce. Weidong Kou, Ed. Springer-Verlag (LNCS series), 2003.

3 A. Herzberg , D. Naor, Surf'N'Sign: client signatures on Web documents, IBM Systems Journal, v.37 n.1, p.61-71, 1997

4 Günther Horn , Bart Preneel, Authentication and Payment in Future Mobile Systems, Proceedings of the 5th European Symposium on Research in Computer Security, p.277-293, September 16-18, 1998

5 MacGregor, R., Ezvan, C, and Liquori, L., Eds. Secure Electronic Transactions: Credit Card

NPL search

BY AMIR HERZBERG

PAYMENTS AND BANKING WITH MOBILE PERSONAL DEVICES

MOBILE DEVICES ENABLE SECURE, CONVENIENT AUTHORIZATION OF E-BANKING, RETAIL PAYMENT, BROKERAGE, AND OTHER TYPES OF TRANSACTIONS.

The growth of mobile commerce follows the increasingly popular ownership and use of mobile personal, programmable communication devices, including mobile phones and PDAs. These devices are effective for authorizing and managing payment and banking transactions, offering security and convenience advantages compared to online payment via PCs. Some of these advantages are available in existing devices, others require modest, inexpensive enhancements likely to be available in new devices in the next few years. The use of secure and convenient mobile personal devices could revolutionize the payment, banking, and investment industries worldwide. Here, I discuss some of the challenges and opportunities involved in their use for making secure payments and authorizing banking transactions.

ILLUSTRATION BY TERRY MIURA

Security and convenience are the two main motivations for using these devices for transactions. The security is revolutionary. Existing means of electronic authorizations, including ATM transactions and card-not-present credit/debit card transactions, as well as online banking, are based on account-holder authentication by the payment system. But it can fail in multiple ways, including through the compromise of the bank's computers and, in online banking, of the user's computer, as well. Computers are generally vulnerable to compromise, especially the user's computer, which typically has minimal security mechanisms and processes. However, existing systems do not always distinguish among fraud by the user, compromise of the user's computer, and compromise of the bank's computer. Assigning responsibility for damages resulting from fraud and disputes is therefore done through administrative and legal means rather than through technical means. In most countries, credit card purchasing, ATM withdrawals, and electronically generated money transfers must be cancelled if the user claims not to have authorized them (and the bank cannot prove the user is cheating). Online brokerage and banking operations are normally irreversible. Responsibility is not necessarily allocated fairly, and non-corrupted, genuinely innocent parties may find themselves responsible for damages due to another party's fraudulent activity or security breach. Moreover, when using online banking and brokerage services, users are vulnerable to attacks on their (insecure) computers, as are the bank's computers. Note that using a smart card connected to the PC does not ensure security, as a corrupted PC (possibly infected by a virus) may send incorrect information to the smart card; a secure transaction device needs its own I/O interface to the user [8]. The lack of a technical solution for preventing and resolving fraud creates substantial risk and expense for users, merchants, and operators (banks) alike.

Mobile personal devices, usually with a built-in display and keyboard, are well-positioned to provide a technical solution for reducing fraud and allowing the fair allocation of responsibility for damages from fraud. Some amount of security is already part of the authentication mechanism of existing cell phones as a way to prevent call theft. Moreover, it is relatively easy and inexpensive for device manufacturers to incorporate additional mechanisms to ensure secure transaction authorization. These mechanisms help prevent most fraud and allocate responsibility fairly for any remaining fraud. For users, their value far outweighs their relatively modest cost.

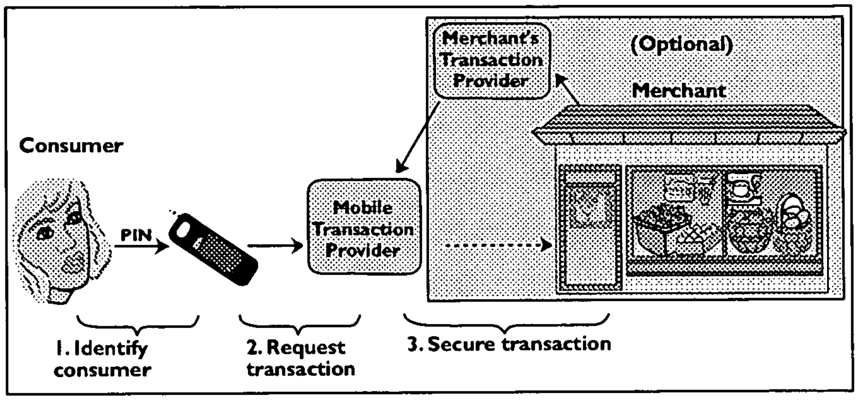


Figure 1. Modular secure transaction architecture using mobile personal devices.

Convenience is another reason people use mobile personal devices for transactions. Convenience can result from using their communication capabilities when paying for goods and services, whether on foot or in cars, planes, or trains, and authorizing transactions at remote servers of banks, brokerages, and merchants.

A device's user interface can also improve convenience; for example, the user can view balances and logs of transactions and retrieve receipts of payments. It also makes it easy for a single mobile device to support several applications, including banking, investment, and retail payments, using multiple charge, micropayment (cash), and loyalty accounts, all supported by a uniform user interface and consolidated management. To support the many possible scenarios and applications, these devices should incorporate modular authorization architectures.

Transactions Architecture

Figure 1 outlines a modular architecture for secure transactions using these devices. Components include at least the user, the device, and a mobile transaction provider, which may be a cellular operator, a bank, or a combination of operator and bank. In a payment transaction, a merchant (a provider of services and/or goods) is also included; however, because the merchant may work with a different transaction provider, the two providers have to be able to interoperate. The arrows represent long-term relationships; the broken arrow represents a transaction-specific relationship.

Secure transactions consist of three independent processes:

Identification. The device identifies the user through physical possession (as with regular cell phones), EXISTING SYSTEMS DO NOT ALWAYS DISTINGUISH AMONG FRAUD BY THE USER, COMPROMISE OF THE USER'S COMPUTER, AND COMPROMISE OF THE BANK'S COMPUTER.

passwords, or biometrics (such as voice recognition);

Authentication. The mobile provider authenticates the transaction request from the device via either subscriber identification (as with existing phones) or cryptographic mechanisms (such as digital signatures or secure protocols, like the Wireless Transport Layer Security Specification) [10]; and

Secure performance. The transaction is performed by the mobile transaction provider, possibly with the help of the merchant and/or other transaction provider(s) and may involve secure payment protocols (such as Internet Keyed Payments/Secure Electronic Transactions, or iKP/SET) [1, 5]; the mobile transaction provider is independent of the communication protocol in the mobile device. For additional modularity, it may use mobile gateway(s) to support multiple communication and authorization mechanisms.

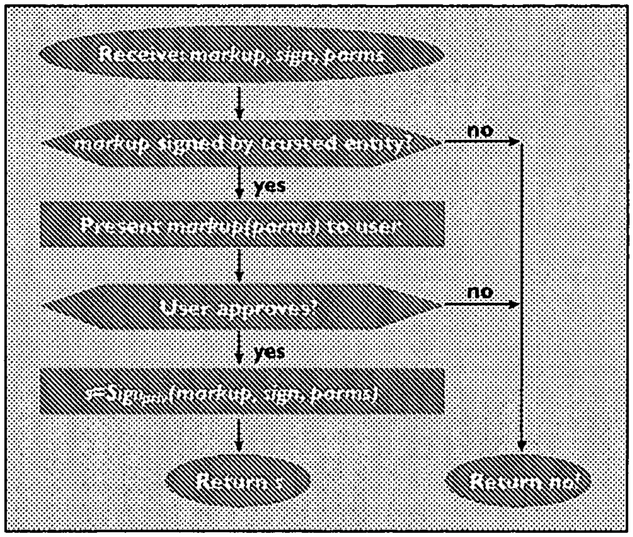

Receive: markup, sign, parms
markup signed by trusted entity?
no
yes
Present markup(parms) to user
User approves?
no
yes
s=Sign_priv(markup, sign, parms)
Return s
Return no!

Figure 2. Secure transaction request by personal mobile device.

This modular design provides inexpensive and flexible support for secure transactions.

Transaction Request Mechanisms

Mobile personal devices should incorporate mechanisms to securely authenticate transaction requests that can be used by (preferably) multiple transactions and scenarios. To allocate responsibility, transaction requests should be digitally signed by the device using a private key (not known to the providers) kept in the device. The user does not have to obtain a public-key certificate from a trusted certificate authority; it suffices that the agreement between the user and the provider states the public key and the algorithm. To reduce hardware costs, designers may prefer public-key signature algorithms (such as the Digital Signature Algorithm, or DSA [7]), so most of the computations are done offline, and online signing is efficient.

The device displays the transaction details to the user and asks his or her consent for each transaction request. The device should ensure the user is aware of the entire request, possibly by limiting the request format; for example, payment transactions may display the amount and other details (such as merchant and product identification).

For flexibility, the device might allow the signing of markup documents using markup language (such as a subset of HTML [3]) with fixed, well-defined rendering. As a further precaution against misleading documents, the device should present to the user and sign upon approval only markup approved or provided by an authority or provider trusted by the user, that is, accompanied by an appropriate signature (and, optionally, by the signer's certificate chain); this allows secure inclusion of identifications and certifications in textual or graphical (trademark) form.

Validating signatures can be computationally intensive (with DSA even more than with the RSA signature-only algorithm). However, most applications need few document templates; a single signed template can be used for many transactions with unsigned values for parameters (such as date, amount, and payee) that differ from transaction to transaction; by caching the (validated) templates, the device can save on both communication and computation overhead. Separating the parameters from the template also simplifies the automated processing of signed transaction requests once they reach the transaction provider. The device signs both the markup and the parameters; to prove the identity of the template approver, this signature may also be included in the data signed by the device (see Figure 2). (Extensions, including those for validating the fairness of lotteries and gambling services, are beyond the scope of this article.)

The security of this design depends on the secure operation of the mobile personal device, including its user identification. Some current mobile devices, including phones, use only simple, preprogrammed processors, and therefore can be trusted to operate securely. However, some devices support downloaded, general-purpose applications and may, like computers, be vulnerable, as with viruses.

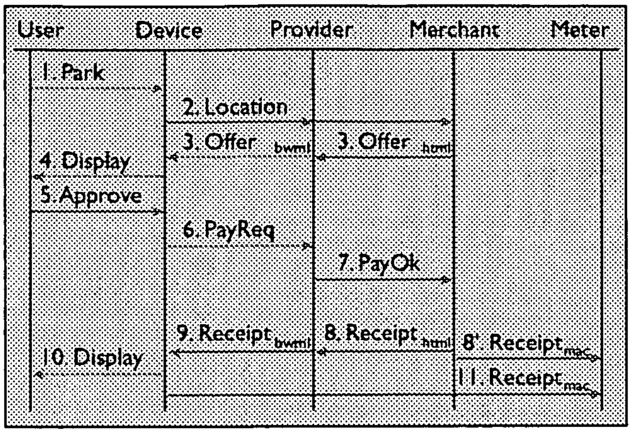


Figure 3. Example of location-based payments using a mobile device.

Secure transaction authorization may, therefore, involve a secure co-processor, used only to authorize transactions (and possibly to view confidential data). There should be visible indication when the display and keyboard are controlled (only) by the secure co-processor, allowing the user to securely identify (such as by password) and authorize transactions. The co-processor is invoked by the main processor to authorize transactions, providing the raw request in shared memory; if authorized, the co-processor returns the signed transaction request in the shared memory.

Applications and Scenarios

The modular secure transaction architecture using mobile personal devices in Figure 1 can be used for multiple applications and scenarios. The simplest involves only the user, the device, and a single transactions provider (such as a bank, brokerage, or insurance company). The user identifies to the mobile device, possibly through secure identification mechanisms (such as a PIN, voice identification, or fingerprint); the device then authorizes a transaction to the provider (such as money transfers and investments). Authorization is preferably through some secure public-key signature process, allowing precise allocation of responsibility for fraud (disputed transactions). However, less secure forms of authorization (such as relying on subscriber identification and/or encrypted passwords) may suffice for some applications, as in e-banking and mobile commerce solutions.

More complex payment transactions typically involve at least one additional party: the merchant. In the simplest case, the merchant receives payment from some arbitrary, external payment/transaction provider (such as a bank or credit card company); the mobile transaction provider authorizes the transaction.

An important payment application is using charge cards to pay remote merchants for, say, goods bought online or on the telephone. Since the merchant and the consumer are in separate locations, the merchant cannot compare the customer's signature to the signature on the charge card. A personal mobile device (such as a cell phone) is an alternative means of validating the customer's consent to the transaction via authenticated communication with the mobile transaction provider. The communication may be initiated by the consumer using the mobile device or by the merchant communicating with mobile transaction providers; for example, in the PayBox system, a merchant (such as a Web site) contacts PayBox, which operates as a mobile transaction provider, and PayBox then contacts the cell phone of the consumer, relying on subscriber identification to trust the reply (approving or rejecting payment). Payment is not guaranteed, since the consumer may dispute the identification. By using secure signature from the consumer's device, instead of subscriber identification, the payment provider or external arbiter can allocate responsibility for fraud, as well as resolve disputes and guarantee payment.

In some scenarios, mobile devices play an additional role beyond authorizing the transaction. Devices used for browsing the Web represent a natural means for paying for goods and services bought through merchants' Web sites. Similarly, mobile devices can initiate location-dependent payments. Figure 3 outlines how a mobile device can be used to pay a parking meter. Imagine the user instructs the device to contact the parking merchant (flow 1). The device then sends its location via the provider to the merchant, initiating the parking transaction (flow 2). The merchant returns the offer; the provider often converts (transcodes) from, say, HTML to binary Wireless Markup Language (WML) the offer to fit the particular mobile device. The offer may contain details relevant to the purchase (such as the "per-fee link syntax" in HTML [6]). The provider also creates markup to display the offer to the user and secure the user's authorization of the transaction request; for the sake of efficiency, this step may be combined with the conversion (transcoding) process.

Using a mobile device with a mechanism for secure transaction requests, the provider sends the offer (flow 3) in signed markup. The device (usually using its secure co-processor) displays the offer to the user, receives approval, and returns (flow 6) a signed transaction request, as in Figure 2.

Employing mobile devices (such as phones) without mechanisms for secure transaction requests, the authorization function has to rely on the security of the communication between the device and the provider. The provider incorporates the offer details (such as amount) into the display markup sent to the device and shown to the user; if the user's response, sent to the provider, is positive (say the user clicks on the link identifying the product and price), the provider views it as transaction authorization. This process requires the provider to link between the offer sent to the mobile device (flow 3) and the payment transaction request received from the mobile device (flow 6). To avoid maintaining state in the provider, the payment request may contain the state information, possibly in a cookie or as parameters of the URL. To prevent forgery or replay, the state includes a Message Authentication Code (MAC) using a key known only to the provider and computed over the state and time.

Upon receiving an authenticated payment transaction request (flow 6), the provider confirms payment to the merchant (flow 7) by sending a signed or authenticated message. The merchant sends a receipt confirming payment was received; if the meter is connected to the merchant's server, it may be sent directly to the meter (flow 8'). More often, the meter has minimal communication capabilities (such as infra-red), and the receipt is sent via the provider and device (flows 8, 9, 11); the user may even have to manually type the receipt into the meter using a keypad. The receipt may have multiple formats as well; the parking meter itself may use a concise receipt format for efficient communication and processing. Moreover, to allow a low-cost parking meter with limited computational resources to validate the receipt, the receipt sent to the meter (flow 11 or 8') uses an efficient MAC with a shared key between the meter and the merchant's server.

Electronic Receipts and Tickets

Additional applications involving this modular transaction architecture, as in Figure 1, can also provide and use secure electronic receipts, or e-receipts, or a proof of payment the consumer presents to a third party or device. Applications include:

- Presenting the e-receipt to a validating/dispensing device to prove payment and receive service or merchandise; the validation device (such as the parking meter in Figure 3) need not communicate directly with the payment transaction provider or merchant's server, so long as it is able to validate the e-receipt;
- Presenting the e-receipt to a third party (such as the Internal Revenue Service for tax purposes or an employer for expense reimbursement);
- Providing "proof of purchase" for warranty service, returns, exchanges, and rebates; and
- Using the e-receipt as an e-ticket, the mobile device holds the receipt (the ticket), presenting it upon inspection at, say, an airport for claiming tickets.

In each of these applications, except the first, the e-receipt should be a digital signature from the payment transaction provider or the merchant, thus allowing validation at arbitrary times by any party.

Payments via Mobile Transaction Provider

The mobile transaction provider may also be involved in the actual payment to the merchant. (Charging by mobile operators for communication and value-added services is a special case.) In today's mobile phones, authorization is via subscriber identification mechanisms, which do not provide non-repudiation. However, in the future, mobile consumers might also use a secure mobile signing device, as in Figure 2, to avoid disputes. This device may allow high-value transactions, as well as paying mobile operators who are not completely trusted (such as when roaming). Mobile communication mechanisms (such as the Global System for Mobile communication, or GSM) allow the foreign (visited) network to authenticate the user with information from the home network. Charging requires prior agreements between the visited and the home networks. Designers of the Universal Mobile Telecommunications System (UMTS) recognized the difficulty of establishing agreements in advance among visited networks and all home networks [4]; thus, UMTS includes mechanisms for dynamic negotiation and setup of roaming agreements between a visited network and a home network [4]. Roaming agreements seek to establish fees and ensure operator trustworthiness. Operators are trusted to deliver payments in time; foreign (remote) operators are also trusted to not overcharge visiting customers.

A secure signing mobile device can prevent fraud (overcharging) by foreign network providers, thereby allowing more automated and variable roaming agreements. Operators can also use the Final Payments protocol discussed in [2] to extend pairwise trust relationships into global trust relationships, allowing automated, secure, low-cost universal roaming.

Other payment scenarios involve mobile transaction providers participating in the payment transaction itself, not just in its authorization. One motivation is to establish new payment networks, possibly involving mobile operators and financial institutions as providers of mobile payment services. Motivations for establishing new payment networks include the exploitation of business opportunities inherent in the billing, customer-service, and technical relationships among mobile users (and devices) and mobile operators. Another is support for low-value payments (micropayments) and final (irreversible) payments, each possibly yielding additional mobile communication services. Micropayments and final payments using mobile devices may enable the purchase of content and services delivered via the network, as well as person-to-person payments and money transfers; the latter represents a substantial opportunity, especially in light of the millions of overseas employees worldwide. Moreover, due to their ability to allocate responsibility for fraud, these new payment networks may lower the cost of transactions (as a percentage of the transaction) for large-value payments and money transfers.

A major challenge for any new payment system is how to achieve a critical mass of merchants, buyers, and transactions needed to justify investment by each of them and ensure a proper level of acceptability; for example, a customer of any mobile provider should be able to buy from any merchant that maintains accounts with most payment transaction providers. One solution for payment transaction providers is to use the Final Payments protocol, allowing interoperability among any provider connected by the transitive closure of all pairwise, provider-to-provider trust and interoperability agreements. For instance, interoperability among mobile payment providers is a feature cited by Fundamo, Inc. (www.fundamo.com) in its payment systems product.

In other cases, the mobile transaction provider is part of an existing payment network, as in a credit card network. The involvement of the mobile provider in a credit card transaction could be as simple as transmission via the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol of credit card details or as complex as a purchase via the iKP/SET protocols [1, 5]. In either case, the mobile provider acts on behalf of the user as a wallet server, as it is located along the route between mobile device and merchant. The mobile transaction provider may implement a variety of payment protocols, ranging from the complex (such as iKP/SET) to the simple (such as SSL/TLS transmission of credit card numbers). The mobile provider may securely inform the credit-card-issuing bank of any pending transaction, allowing the issuer to reject fraudulent transactions; a one-time or limited (to payments via mobile provider) card number may be used for added security.

Conclusion

Mobile personal devices are beginning to be used to perform secure banking, payment, and other transactions. Cell phones, PDAs, and other mobile personal devices are a convenient means for authorizing transactions. In the future, they are likely to incorporate low-cost enhancements providing secure, signed transaction requests, providing third-party verifiable proof of the consumer's agreement to each transaction. This support will be flexible enough to support multiple applications, scenarios, and providers. New payment networks are likely to take advantage of the new capabilities, offering such services as micropayments and final payments previously impossible or impractical. Mobile personal devices will play an increasingly important role in payments, banking, investing, and other transaction-based and security-sensitive applications.

References

1. Bellare, M., Garay, J., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Van Herrenweghen, E., and Waidner, M. Design, implementation, and deployment of the iKP Secure Electronic Payment System. *J. Select. Areas Commun. 18*, 4 (Apr. 2000), 611–627.
2. Herzberg, A. Micropayments. In *Advances in Payment Technology for E-commerce*. Weidong Kou, Ed. Springer-Verlag (LNCS series), 2003.
3. Herzberg, A. and Naor, D. Surf'N'Sign: Client signatures on Web documents. *IBM Syst. J. 37*, 1 (Jan. 1998), 61--71.
4. Horn, G. and Preneel, B. Authentication and payment in future mobile systems. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS'98) Lecture Notes in Computer Science* (Louvain-la-Neuve, Belgium, Sept. 6–8). Springer Verlag, 1998, 277–293.
5. MacGregor, R., Ezvan, C, and Liquori, L., Eds. *Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice*. SG24-4978-00 Redbook, IBM, International Technical Support Organization, Raleigh, NC, July 2, 1997; see www.redbooks.ibm.com/.
6. Michel, T., Ed. *Common Markup for Micropayment Per-Fee Links*. W3C Working Draft, Aug. 25, 1999; see www.w3.org/TR/Micropayment-Markup.
7. National Institute of Standards and Technology (NIST). *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication FIPS 186. U.S. Department of Commerce, Washington, DC, May 1994.
8. Pfitzmann, A., Pfitzmann, B., Schunter, M., and Waidner, M. Trustworthy user devices. In *Multilateral Security in Communications*, G. Muller and K. Rannenberg, Eds. Addison-Wesley, 1999, 137–156.
9. Rescorla, E. *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2000.
10. The WAP Forum. *WAP-199, Wireless Transport Layer Security Specification*; see WAP-199-WTLS-20000218-a.pdf.

AMIR HERZBERG (amir@herzberg.name) is an associate professor in the Computer Science Department at Bar-Ilan University, Ramat Gan, Israel.

18	197	((delet$3 or remov$3 or cancel$5) near2 ("electronic receipt" or "electronic receipts" or receipt$1)) and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 20:56
19	6	((delet$3 or remov$3 or cancel$5 or updat) near2 ("electronic receipt" or "electronic receipts" or receipt$1)) and ("electronic receipt" or "electronic receipts") and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:26
23	283	((delet$3 or updat) near5 ("electronic receipt" or "electronic receipts" or receipt$1)) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:28
24	106	((delet$3 or updat) near2 ("electronic receipt" or "electronic receipts" or receipt$1)) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:31
25	1	((delet$3 or updat) near2 ("electronic receipt" or "electronic receipts")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:31
26	7	((delet$3 or updat) same ("electronic receipt" or "electronic receipts")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:38
27	1	((delet$3 or updat) adj5 ("electronic receipt" or "electronic receipts")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:56
28	1	((delet$3 or updat) adj5 ("electronic receipt" or "electronic receipts" or "e-receipt" or "e-receipt")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:56
29	8	((delet$3 or updat) same ("electronic receipt" or "electronic receipts" or "e-receipt" or "e-receipt")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 22:16
30	8	((delet$3 or updat) same ("electronic receipt" or "electronic receipts" or "e-receipt" or "e-receipts")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 22:16
31	30	((warrant$3 or upgrade$1 or recall$ or update$ or exchange!) same ("electronic receipt" or "electronic receipts" or "e-receipt" or "e-receipts")) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 22:20
32	30	((warrant$3 or upgrade$1 or recall$ or update$ or exchange!) same ("electronic receipt" or "electronic receipts" or "e-receipt" or "e-receipts")) and ("electronic receipt" or "electronic receipts" or "e-receipt" or "e-receipts") and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 22:41
33	4	5047614.pn. 5250789.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 22:42

L Number	Hits	Search Text	DB	Time stamp
1	0	707/10.ccls. and (("electronic receipt" or "electronic receipts") same purchas$5) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 16:32
2	82	(("electronic receipt" or "electronic receipts") same purchas$5) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 18:42
3	34	((("electronic receipt" or "electronic receipts") same purchas$5) and @ad<20010809) and profile$2	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 16:50
4	2	6193152.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 18:34
5	4	6193152.pn. 5509071.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 20:45
6	0	(6193152.pn. 5509071.pn.) and (search$3 or quer$3 or retriev$)	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 18:38
7	63	((("electronic receipt" or "electronic receipts") same purchas$5) and @ad<20010809) and (search$3 or quer$3 or retriev$)	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 18:38
9	3	(search$3 or quer$3 or retriev$) near2 ("electronic receipt" or "electronic receipts") and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 18:59
8	19	(search$3 or quer$3 or retriev$) same ("electronic receipt" or "electronic receipts") and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 18:46
11	3	(search$3 or quer$3 or retriev$) near2 ("electronic receipt" or "electronic receipts") and ("electronic receipt" or "electronic receipts") and (search$3 or quer$3 or retriev$) and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 19:26
12	1	(delet$3 near2 ("electronic receipt" or "electronic receipts")) and ("electronic receipt" or "electronic receipts") and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 19:40
13	7	(delet$3 same ("electronic receipt" or "electronic receipts")) and ("electronic receipt" or "electronic receipts") and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 19:43
14	30	(delet$3 same ("electronic receipt" or "electronic receipts" or receipt$1)) and ("electronic receipt" or "electronic receipts") and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 19:43
15	3	(delet$3 near2 ("electronic receipt" or "electronic receipts" or receipt$1)) and ("electronic receipt" or "electronic receipts") and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 20:46
16	0	6193152.pn. and delet	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 20:45
17	6	((delet$3 or remov$3 or cancel$5) near2 ("electronic receipt" or "electronic receipts" or receipt$1)) and ("electronic receipt" or "electronic receipts") and delet$3 and @ad<20010809	USPAT; US-PGPUB; EPO; JPO; DERWENT	2003/12/12 21:17

US006487540B1

(12) United States Patent

Smith et al.

(10) Patent No.: **US 6,487,540 B1**

(45) Date of Patent: **Nov. 26, 2002**

(54) **METHODS AND SYSTEMS FOR ELECTRONIC RECEIPT TRANSMISSION AND MANAGEMENT**

(75) Inventors: **Steven B. Smith**, Holladay, UT (US); **Nicolas A. Thomas**, Orem, UT (US); **Warren M. Rosner**, South Jordan, UT (US)

(73) Assignee: **In2M Corporation**, South Jordan, UT (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 41 days.

(21) Appl. No.: **09/625,141**

(22) Filed: **Jul. 25, 2000**

(51) **Int. Cl.**^{7} **G60F 1/12**; G60F 17/60

(52) **U.S. Cl.** **705/21**; 705/24

(58) **Field of Search** 705/21, 24

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,821,513 A	* 10/1998	O'Hagan et al.	....	235/383
6,029,150 A	2/2000	Kravitz	....	705/39
6,039,250 A	3/2000	Ito et al.	....	235/380
6,049,786 A	4/2000	Smorodinsky	....	705/40
6,058,373 A	5/2000	Blinn et al.	....	705/26
6,067,529 A	* 5/2000	Ray et al.	....	705/26
6,250,557 B1	* 6/2001	Forslund et al.	....	235/492

FOREIGN PATENT DOCUMENTS

EP	0 474 360	* 3/1992
WO	WO 99/16029	* 4/1999

OTHER PUBLICATIONS

"Retail systems: no longer business as usual" by Steven J. Johnson, Journal of Systems Management, v43, n8, p8(5), Aug., 1992, ISSN: 0022-4839.*

"Networks in the mall" by Lisa Terry, LAN Magazine, v9, n7, p133(4), Jul. 1994, ISSN: 0898-0012.*

* cited by examiner

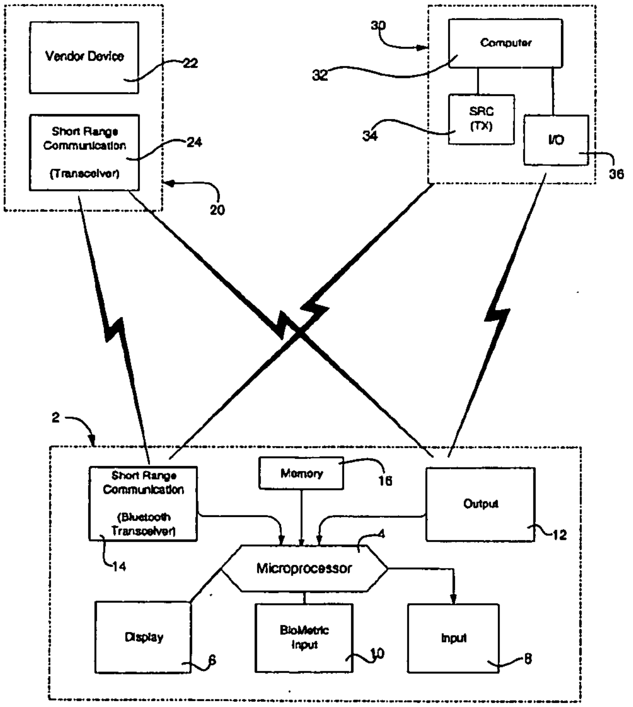
Primary Examiner—Kenneth R. Rice

(74) *Attorney, Agent, or Firm*—Kirton & McConkie; Michael F. Krieger

(57) **ABSTRACT**

Embodiments of the present invention relate to systems, methods and apparatus for the generation, transmission, storage and manipulation of electronic receipts which communicate itemized purchase transaction information. Preferred embodiments comprise wireless vendor devices and wireless purchaser devices which transmit electronic receipts at a point-of-sale for documentation of a purchase transaction. Further processing of the electronic receipt information may be performed with a purchaser device or with a secondary computing device after subsequent receipt transmission to that secondary device.

16 Claims, 3 Drawing Sheets



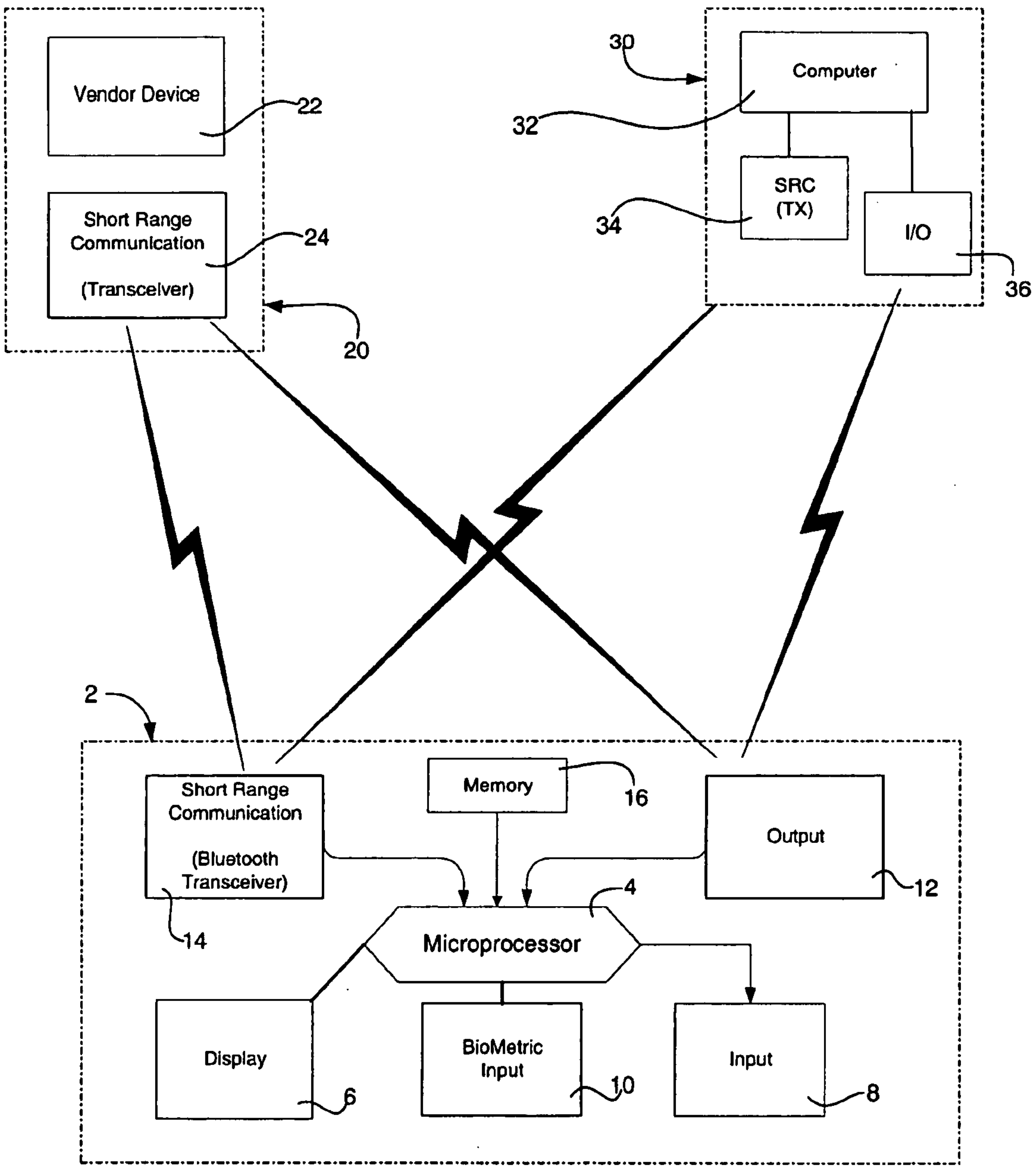

Vendor Device
22
Short Range
Communication
(Transceiver)
24
20
30
Computer
32
SRC
(TX)
34
I/O
36
2
Short Range
Communication
(Bluetooth
Transceiver)
14
Memory
16
Output
12
4
Microprocessor
Display
6
BioMetric
Input
10
Input
8

Figure 1

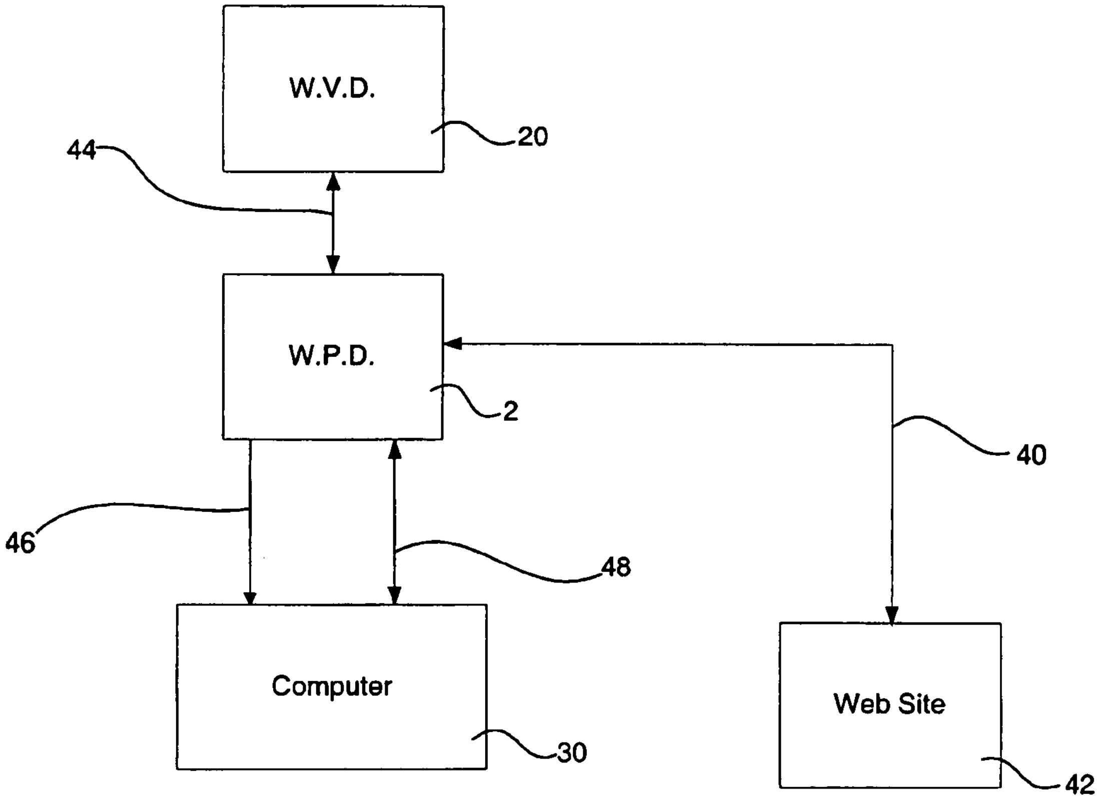


Figure 2

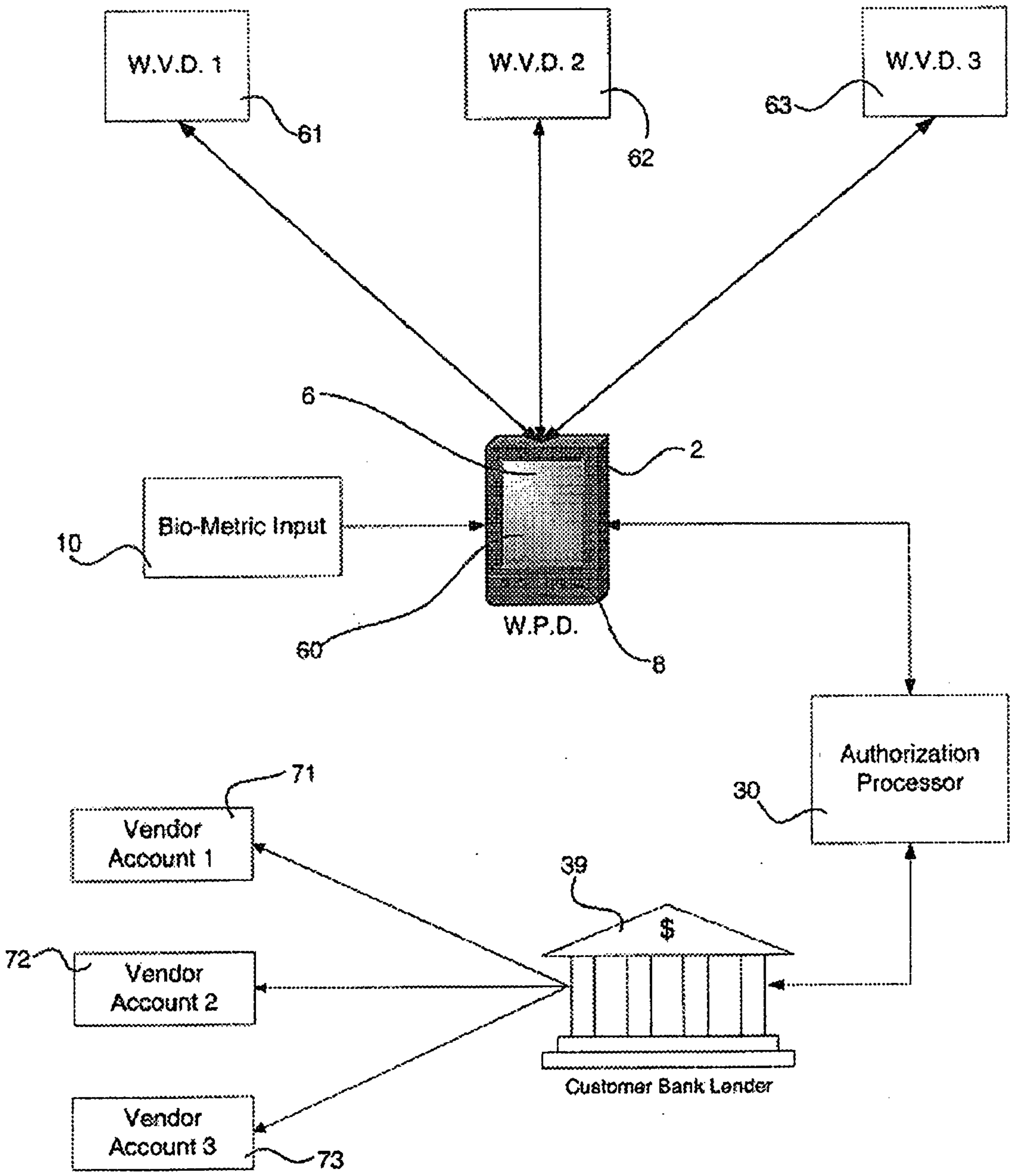

W.V.D. 1
61
W.V.D. 2
62
W.V.D. 3
63
6
2
10
Bio-Metric Input
60
W.P.D.
8
Authorization Processor
30
71
Vendor Account 1
39
$
72
Vendor Account 2
Customer Bank Lender
Vendor Account 3
73

Figure 3

METHODS AND SYSTEMS FOR ELECTRONIC RECEIPT TRANSMISSION AND MANAGEMENT

THE FIELD OF THE INVENTION

Embodiments of the present invention relate to methods, systems and apparatus for communication and management of electronic receipt information. More particularly, these embodiments provide for the transmission of an electronic receipt from a vendor device to a purchaser device and for subsequent transmission, in some embodiments, of the electronic receipt to management and accounting software. An electronic receipt may be transmitted in conjunction with cash payment, charge, debit and authorization information or may be transmitted as a unique entity. Some embodiments of the present invention may utilize wireless purchasing devices (WPDs) to communicate with point-of-sale wireless vendor devices (WVDs) and arrange the electronic transfer of receipt information.

BACKGROUND

Electronic transactions involving the transfer of money and pecuniary assets are common in our society today. Stocks and bonds may be purchased and traded using only electronic transactions. Goods and services are also commonly purchased over the telephone or via the Internet using credit or debit accounts with electronic authorization.

Retail vendors typically accept credit and debit cards which are verified and authorized using electronic communications methods. Nearly every significant retail vendor accepts some form of credit or debit card as remuneration for goods or services. The accounts accessed through these cards are typically identified by a number embossed on the card and a magnetic strip on the card's surface that is encoded with account information. Transactions involving a credit or debit card account require authorization from the organization who issues the card. This authorization is generally obtained at the point-of-sale by a vendor through electronic communications channels. A transaction amount is determined and the amount of the transaction along with the account identification information are transmitted to the organization which issued the card or an authorization provider(AP). If the account has sufficient credit or finds to cover the transaction amount and the account has not been deactivated for some other reason, the card issuer will send an authorization code to the vendor or AP which indicates that the issuer will transfer the authorized amount to the vendor at an appropriate time.

Account information may be obtained by swiping the electronic strip of the card across a magnetic reader thereby eliminating the need for manual input. The transaction amount may also be transferred from an electronic cash register and combined with the account information automatically to make an authorization request.

These point-of-sale authorization request devices are typically connected to the card issuers or their representatives, sometimes known as authorization processors (APs), through a conventional telephone line. Often a dedicated phone line is connected to the point-of-sale authorization device for quick access to authorization data.

Wireless communication technology has progressed rapidly in recent years. Cell phones and other long-range communication devices have proliferated and are now commonplace among consumers. As technology advances, the cost of these devices is plummeting and even more widespread use is eminent. Mobile phones, pagers, two-way radios, smartphones, personal digital assistants (PDAs) and other communicators are all available on the market.

Internet use is also skyrocketing with millions of new users logging on each year. Internet commerce now represents a significant portion of retail commerce and is used by millions of consumers each day.

Communications protocols exist which allow present generation electronic communications devices to interface with the Internet and access Internet resources. The Wireless Application Protocol (WAP) is an open, global specification that enables mobile wireless communications devices to access and interact with Internet information and services. WAP is a communications protocol and environment which can be built on nearly any operating system including PalmOS, EPOC, Windows CE, FLEXOS, OS/9, JavaOS and others and provides service interoperability between different device families. WAP works with most existing wireless communications networks such as CDPD, CDMA, GSM, PDC, PHS, TDMA, FLEX, ReFLEX, iDEN, TETRA, DECT, DataTAC, Mobitex and others. WAP developers operate Internet gateways specifically tailored for wireless communications device users. These devices typically have small displays, limited memory and less bandwidth that stationary, wire connected computers, therefore, WAP provides for use of eXtended Markup Languages (XMLs) such as the Wireless Markup Language (WML) which offers Internet content tailored for cell phones, PDAs and other wireless, portable communications devices.

Using WAP and similar technologies, vendors, news agencies, financial institutions and other providers allow cell phone and other portable communications device users to buy and sell securities, execute credit card transactions, make account transfers, make bill payments, receive and send e-mail, view news reports. These providers offer seamless integration between the Internet and wireless portable communication devices.

Wireless communication devices are also becoming commonplace in the electronics industry. Wireless networking of portable computers and associated devices is now replacing a large segment of the networking market. Wireless communication devices including wireless networking adapters, hubs and other equipment utilize radio transmitters and receivers to transmit data signals from one device or node to another. These radio transmitters and receivers must utilize a specific frequency band and protocol to accomplish this task. Since these wireless networks and communications areas may often overlap, standards, protocols and privacy protection are necessary. One current standard in the industry has been established by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and is known as IEEE 802.11. This standard comprises communications standards, protocol and equipment specifications for wireless communication equipment including privacy and encryption provisions.

Another innovation in the wireless communications arena is the advent of short-range wireless networking between portable communications devices. One standard for this technology is known as Bluetooth®, and is being established by a collaborative group of communications and computing companies. Devices incorporating Bluetooth® technology will utilize a micro-chip transceiver for communications between devices. Bluetooth® devices will transmit in the previously unused 2.4 GHz range and will have a range of about 10 meters which may be extended to about 100 meters by increasing transmitter power. Bluetooth® technology promises to be a viable and economical networking solution for interconnection of cell phones, computers, printers, modems, computer peripherals, fax machines and other communications and computing devices. The size of the Bluetooth® transceiver makes it usable in devices as small as palm computers and cell phones.

Another established wireless connectivity standard is known as IrDA and employs infrared radiation to communicate between devices. IrDA is a point-to-point narrow angle, ad-hoc data transmission standard designed to operate over a distance of 0 to 1 meter at speeds of 9600 bps to 16 Mbps. It is typically used in a point-and-shoot fashion by pointing one device at another for direct data transmission.

SUMMARY AND OBJECTS OF THE INVENTION

Preferred embodiments of the present invention provide systems, methods and apparatus which provide for the generation, transmission and management of electronic receipts. Electronic receipts of embodiments of the present invention may comprise purchase transaction information including, but not limited to, total purchase price, vendor ID, purchaser ID, item descriptions, itemized pricing, purchase date, purchase time, discount information, creditor information, authorization information, receipt management information and other transaction information. The electronic receipts of embodiments of the present invention comprise itemized information so that detailed tracking and accounting of purchased items may be performed automatically.

automatic

Typically, an electronic receipt will be generated by a vendor device at a point-of-sale. When a transaction takes place, an electronic receipt may be transmitted from the vendor device to a purchaser device where the receipt may be stored for further processing within the device or for further transmission to other devices and systems. Preferred embodiments of the present invention employ a wireless vendor device (WVD) which may be a single device or a combination of devices capable of generating receipt information and transmitting receipt information to other devices. A WVD typically employs wireless communications technology to transmit the receipt information. Embodiments of the present invention may employ a radio frequency transmitter, an Infrared transmitter or other wireless communications methods.

The electronic receipt will generally be transmitted to a purchaser device and, in preferred embodiments, to a wireless purchasing device (WPD) which can store and manipulate the electronic receipt. A purchaser device, such as a WPD, may process and display the electronic receipt information directly as well as retransmit the receipt information to other devices or systems for further processing. A WPD may take the form of a personal digital assistant (PDA), a wireless phone or some other wireless communication device.

Alternate scenarios include purchasing an item using a wireless point of sale system. With this transaction, receipt is transferred from the vendor to the wireless point of sale device over a wireless system such as Bluetooth_{13} or IrDA connection. Under this scenario no direct Internet connection is required as the information is transferred directly over a wireless connection over the WPD and the vendor.

Another purchasing scenario involves the purchasing of an item over a direct Internet connection via an Internet Protocol. For example, WAP. In this purchasing scenario, receipt is transferred from the vendor to the WPD via a wired or a wireless Internet connection.

Once the electronic receipt information has been transmitted to the purchaser device, the information derived from the electronic receipt may be processed and manipulated to provide additional functionality. Preferred embodiments of the present invention employ processing methods which compile multiple electronic receipts and provide a user with an accounting of each item purchased along with purchase information. Items listed in electronic receipts may be categorized into categories of items for accounting purposes. Each item on an electronic receipt may be placed in one or more categories and each item may be related to specific budget accounts. The methods of embodiments of the present invention may provide for real-time budgeting and accounting processes which allow a user to be constantly aware of current account and budget situations.

Accordingly it is an object of some embodiments of the present invention to provide systems, method and apparatus for creating electronic receipts.

It is another object of some embodiments of the present invention to provide systems methods and apparatus for transmitting electronic receipts.

It is yet another object of some embodiments of the present invention to provide systems methods and apparatus for providing accounting and budgeting methods using electronic receipts.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above-recited and other advantages and objects of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

FIG. 1 is a diagram showing components of a preferred embodiment of the present invention;

FIG. 2 is a diagram illustrating the typical use of an embodiment of the present invention with a single WVD and WPD; and

FIG. 3 is a diagram illustrating an embodiment of the present invention that includes multiple WVDs and multiple vendor accounts.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The figures listed above are expressly incorporated as part of this detailed description.

It will be readily understood that the components of the present invention, as generally described and illustrated in the figures herein, could be arranged and designed in a wide variety of different configurations. Thus, the following more detailed description of the embodiments of the system and apparatus of the present invention, as represented in the corresponding drawings, is not intended to limit the scope of the invention, as claimed, but it is merely representative of the presently preferred embodiments of the invention.

The currently preferred embodiments of the present invention will be best understood by reference to the drawings, wherein like parts are designated by like numerals throughout.

In reference to FIG. 1, a preferred embodiment of a consumer's wireless purchasing device (WPD) 2 is shown comprising a microprocessor 4 for processing consumer input, communications functions and display functions as well as other functions. WPD 2 may also comprise a display 6 in preferred embodiments, however display 6 is not required for rudimentary embodiments. An input device 8 may also be part of WPD 2 to allow for consumer input and selection. WPD 2 may communicate with other electronic devices using a short-range communications device 14. Short range communications device 14 may be used to communicate with a vendor's point-of-sale device, such as wireless vending device (WVD) 20, with other WPDs, with external communication devices or with other electronic devices. However, the key function of short range communications device 14 is to communicate with WvDs and to receive electronic receipt information therefrom. Short range communications device 14 may be a Bluetooth® transceiver or similar short range networking device or may be an Infrared transceiver such as an IrDA standard port as well as other devices. WPD 2 also comprises memory 16 for storing electronic receipt and other information. WPD 2 may also comprise input/output (I/O) 12 such as a serial port, parallel port, USB port or some other wired communication connection. I/O 12 may also be used to communicate with a vendor device at a point-of-sale transaction when wireless communication is not available or desired.

Some embodiments of WPD 2 may also comprise a biometric input device 10 to verify user identity. Biometric input device 10 may use thumb print analysis, retinal scan analysis or another identification method to identify the WPD user. Once the user is identified, user identity can be matched to account data to ensure that unauthorized users do not gain access to sensitive information or other user's accounts.

Embodiments of the present invention also comprise a wireless vendor device (WVD) 20 which is typically positioned at a point-of-sale for communication with WPDs. WVD 20 will generally comprise a short range communications device 24 configured to communicate with short range communications device 14 used in WPDs. As with communications device 14, device 24 may be a Bluetooth® transceiver, an IrDA port or another communications device. In situations where multiple vendors are accessible to a single WPD at the same time, a Bluetooth® transceiver or similar networking device is preferred to allow multiple party communications. Short range communications device 24 is connected to a vendor device 22 which is typically an electronic computing device such as an electronic cash register, an electronic vending machine, a bar-code reader or other device which may transmit and receive product and transaction information and transmit electronic receipt information. WVD 20 may communicate electronic receipt information or other information via short range transceiver 24 or via direct cable connection to WPD input/output 12 for direct wireline communications.

WPD 2 may also communicate with secondary computing device 30 which may comprise a variety of devices including, but not limited to, a desktop computer, a mainframe computer, a storage device, a network server, an Internet site and many other computing devices. Secondary computing device 30 may be used for storage and processing of electronic receipt information. When WPD 2 has limited processing ability, limited display capability, limited memory or other limited features, secondary computing device 30 may receive information from WPD 2 for processing, display, storage, conversion or other manipulation or use. Even when WPD 2 does not have limited features, information may be transmitted to secondary computing device 30 for archival storage, redundant file maintenance or any other reason.

WPD 2 may communicate with secondary computing device 30 via a short range communication devices 34 & 14 or by direct wireline link through input/output devices 12 & 36. Input/output devices 12 & 36 may comprise modems, network adapters, serial ports, parallel ports, USB ports and any other communications adapters or connections.

During use of the systems and methods of embodiments of the present invention an exchange of information 44 takes place between a vendor device such as a WVD 20 and a purchaser device such as a WPD 2 as shown in FIG. 2. This information exchange 44 may comprise multiple transactions and multiple bi-lateral or unilateral data transmissions. In some embodiments, information exchange 44 may comprise credit or debit account identification and authorization as well as identification of vendor and purchaser along with account information. Some or all of information exchange 44 may be encrypted, coded or otherwise manipulated to preserve privacy.

Information exchange 44 also comprises the transmission of electronic receipt information from vendor device 20 to purchaser device 2. Electronic receipt information typically comprises purchase transaction information including, but not limited to, total purchase price, vendor ID, purchaser ID, item descriptions, itemized pricing, purchase date, purchase time, discount information, creditor information, authorization information, receipt management information and other transaction information. The electronic receipts of embodiments of the present invention comprise itemized information so that detailed tracking and accounting of purchased items may be performed automatically. Detailed tracking as well as itemized information, automated logging or indexing of stored receipts is also made available.

Information stored in purchaser device 2 may be compiled, displayed, converted or otherwise manipulated within purchaser device 2 through the use of microprocessor 4, memory 16 and other components. Generally, a user may combine receipt information to obtain a running total of itemized and categorized purchase and budget information. When purchaser device 2 has limited processing capabilities or for other reasons, a user may transfer 46 receipt information from purchaser device 2 to secondary computing device 30 for further processing, storage, archiving and other functions.

In a preferred embodiment, secondary computing device 30 is a web server 42 which can be accessed through a wireless Internet connection. Web server 42 may provide compiled receipt information including itemized and categorized purchase and budget information. Web server 42 may further provide banking, automated bill payment, tax preparation and other financial services in connection with receipt information management.

Secondary computing device 30 such as a home computer or web server may also transmit compiled information 48 back to purchaser device 2 for display and reference while a user is unable to connect to secondary computing device 30.

The electronic receipt information of preferred embodiments of the present invention comprises detailed information in an itemized format so that purchase data can be tracked, stored, and compiled for specific purchase items. Items may also be assigned to certain categories for which aggregate information may be compiled. Items may also be assigned to budget accounts from which funds are drawn when those items are purchased. A user may be alerted to budget account overdrafts when receipt information is received or, in some embodiments, a preliminary receipt may be transmitted from vendor device **20** to purchaser device **2** for budget authorization prior to a final purchase transaction. Upon budget approval a specific purchase may be authorized and a final purchase receipt will be transmitted.

Preferred embodiments of an electronic receipt will have complete file integrity so that users may be assured of accurate receipt information regardless of the location or possession of an electronic receipt file. File integrity may be preserved through independent transmission and storage of original receipt information by an independent verification service or by other data integrity preservation methods.

Turning now to FIG. **3**, a customer bank lender **39** is shown handling various vendor accounts **71**, **72**, and **73**, debiting and crediting those accounts as authorization is received. An authorization processor **30** takes requests from devices such as wireless purchasing device **2** and either forwards an authorization and response to the request or forwards a denial. If the request cannot be satisfied either because of insufficient finds or some other inconsistency in the process, then a denial is forwarded to the wireless purchasing device. The request forwarded by the wireless purchasing device **2** are received from wireless vending devices **61**, **62**, and **63**. The system may operate using several scenarios. For example, in one scenario, the owner of a wireless purchasing device 2 would place an order from wireless vending device **61**. Before the order is transmitted to wireless vending device **61**, the proper ownership of the device could be verified through biometric input **10**. Once verified, the order could be transmitted wirelessly to the wireless vending device whereupon the device would respond by indicating that there were sufficient quantities of product available at the price requested and would transmit that information back to the wireless purchasing device along with an authorization code. The wireless purchasing device would then forward the authorization code in a request to the authorization processor **30**. Authorization processor **30** would then locate the appropriate customer bank lender **39** and forward the request for transfer of funds. The customer bank lender would use the authorization code to locate the correct vendor account and it would transmit funds from the owner of the wireless purchasing device over into the account of the vender. Once the funds have been transferred, a transfer verification would be forwarded back to the authorization processor back to wireless purchasing device **2** and forwarded to wireless vending device **61**. Upon receiving the verification, the vending device would release the product to the owner of the wireless purchasing device. It should be understood that the wireless vending device **61** is used only as an example and that purchases can also be made from any number and type of vendors.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrated and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

We claim:

1. A system for use in a wireless purchasing environment wherein an electronic receipt is generated by a purchaser-owned device at a point of sale, the system comprising:

a wireless vendor device configured to provide product information to the purchaser-owned device;

a remote authorization processor configured to wirelessly receive an authorization request from the purchaser-owned device, to transmit authorization information to the purchaser-owned device, and to transmit the authorization information to a bank lender to effect a transfer of funds; and

the wireless purchaser-owned device configured to send and receive short range communications with the wireless vendor device, to send a long range authorization request to the authorization processor, and to receive the authorization information from the authorization processor, wherein the purchaser-owned device is further configured to store the authorization information received from the authorization processor and to transmit the authorization information to the vendor device to effect the purchase of a product or service.

2. A system as recited in claim **1**, wherein the wireless purchaser-owned device comprises a biometric input device to identify a user.

3. A system as recited in claim **1**, wherein the purchaser-owned device is configured to selectively manage the authorization information with other authorization information corresponding to other purchases made.

4. A system as recited in claim **1**, wherein the purchaser-owned device is a pda.

5. In a wireless purchasing environment wherein an electronic receipt is generated by a purchaser-owned device at a point of sale, a method for effecting a purchase of a product or service, the method comprising the steps for:

obtaining sales information from a wireless vendor;

sending a long range authorization request from a wireless purchaser-owned device to an authorization processor;

receiving authorization information at the wireless purchaser-owned device from the authorization processor; and

transmitting the authorization information from the wireless purchaser-owned device to the wireless vendor device to effect the purchase.

6. A method as recited in claim **5**, further comprising the steps for:

receiving biometric information at the purchaser-owned device; and

using the biometric information at the purchaser-owned device to identify a user.

7. A method as recited in claim **5**, further comprising the step for storing a copy of the authorization information at the purchaser-owned device.

8. A method as recited in claim **7**, further comprising the step for managing the copy of the authorization information and other authorization information on the purchaser-owned device that corresponds to other purchases.

9. A method as recited in claim **5**, wherein the wireless purchaser-owned device is a pda.

10. In a wireless purchasing environment wherein an electronic receipt is generated by a purchaser-owned device at a point of sale, a method for providing authorization to effect a purchase, the method comprising the steps for:

receiving, at an authorization processor, a long-range authorization request from a wireless purchaser-owned device;

transmitting authorization information from the authorization processor to the wireless purchaser-owned device to enable the wireless purchaser-owned device to provide the authorization information to a wireless vendor device to effect the purchase; and

transmitting a copy of the authorization information to a corresponding bank lender to effect a transfer of funds corresponding to the purchase.

11. A method as recited in claim **10**, wherein the authorization request includes information identifying a user of the purchaser-owned device.

12. A method as recited in claim 11, wherein the identification information includes biometric information of the user.

13. A method as recited in claim 11, wherein the authorization request further includes vendor information provided by the vendor device to the purchaser-owned device.

14. A method as recited in claim 10, further comprising the step for transferring the funds from a first account to a second account.

15. A method as recited in claim 14, wherein the first account is owned by the purchaser and the second account is owned by the vendor.

16. A method as recited in claim 10, wherein the wireless purchaser-owned device is a pda.

* * * * *

US006394341B1

(12) United States Patent
Mäkipää et al.

(10) **Patent No.: US 6,394,341 B1**
(45) **Date of Patent: May 28, 2002**

(54) **SYSTEM AND METHOD FOR COLLECTING FINANCIAL TRANSACTION DATA**

(75) Inventors: **Mikko Mäkipää** ; **Olli Immonen**, both of Helsinki (FI)

(73) Assignee: **Nokia Corporation**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/382,354**

(22) Filed: **Aug. 24, 1999**

(51) **Int. Cl.**^{7} **G06F 17/60**
(52) **U.S. Cl.** **235/379**; 235/380; 380/24
(58) **Field of Search** 235/379, 380, 235/383, 462.46, 472.02; 705/39, 40, 41, 44; 380/24

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,277,837	A	*	7/1981	Stuckert	235/379
5,221,838	A	*	6/1993	Gutman et al.	235/379
6,091,817	A	*	7/2000	Bertina et al.	380/9
6,142,369	A	*	11/2000	Jonstromer	235/379
6,202,054	B1	*	3/2001	Lawlor et al.	705/42

FOREIGN PATENT DOCUMENTS

GB	2320354	*	6/1998	235/379

* cited by examiner

Primary Examiner—Karl D. Frech
Assistant Examiner—Daniel St. Cyr
(74) *Attorney, Agent, or Firm*—Antonelli, Terry, Stout & Kraus, LLP

(57) **ABSTRACT**

The present invention is a system and method for collecting transaction data. A system for collecting transaction data in accordance with the invention includes at least one transaction provider (**12**) which provides at least an electronic receipt of financial transactions offered by each transaction provider; at least one user device (**14**), in communication with each transaction provider, which provides to each transaction provider a selection by a user of the user device of an offered financial transaction and in response to receipt of an acceptance of the financial transaction recorded in the received electronic receipt; and at least one user information system (**18**), coupled to at least one of the at least one transaction provider or the at least one user device, which stores at least electronic receipts which are received from the at least one user device or the at least one transaction provider which are verified by the user information system to have been accepted by the user of the user device. At least one intermediate service provider (**20**) may be coupled to the at least one transaction provider processes information relating to the accepted financial transactions transmitted to the at least one intermediate service provider to produce processed information pertaining to the accepted financial transactions.

79 Claims, 9 Drawing Sheets

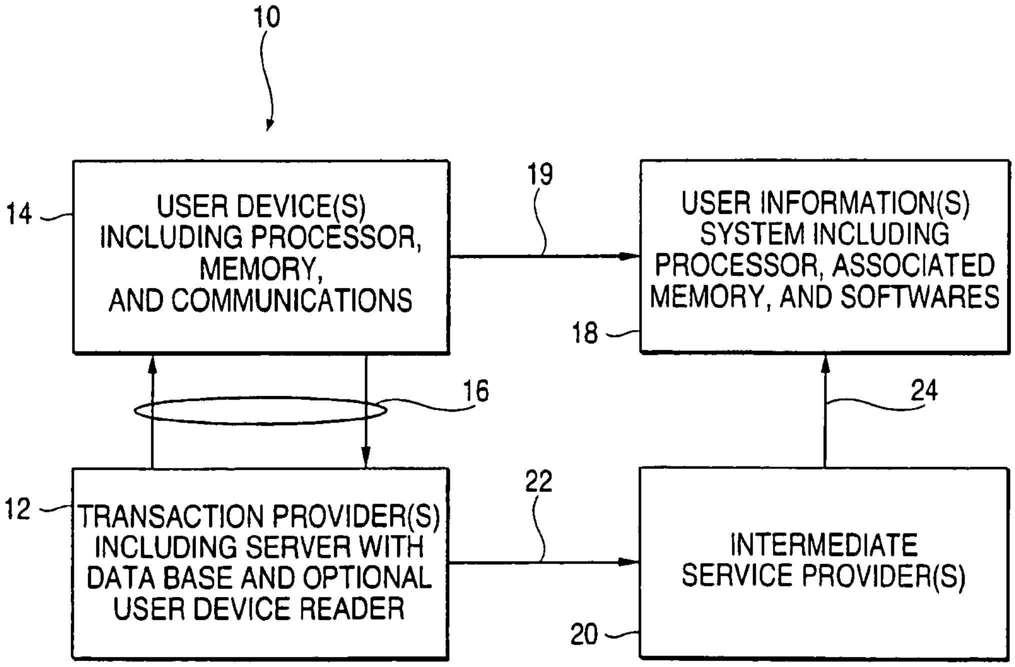

10
14
USER DEVICE(S) INCLUDING PROCESSOR, MEMORY, AND COMMUNICATIONS
19
USER INFORMATION(S) SYSTEM INCLUDING PROCESSOR, ASSOCIATED MEMORY, AND SOFTWARES
18
16
24
12
TRANSACTION PROVIDER(S) INCLUDING SERVER WITH DATA BASE AND OPTIONAL USER DEVICE READER
22
INTERMEDIATE SERVICE PROVIDER(S)
20

FIG. 1

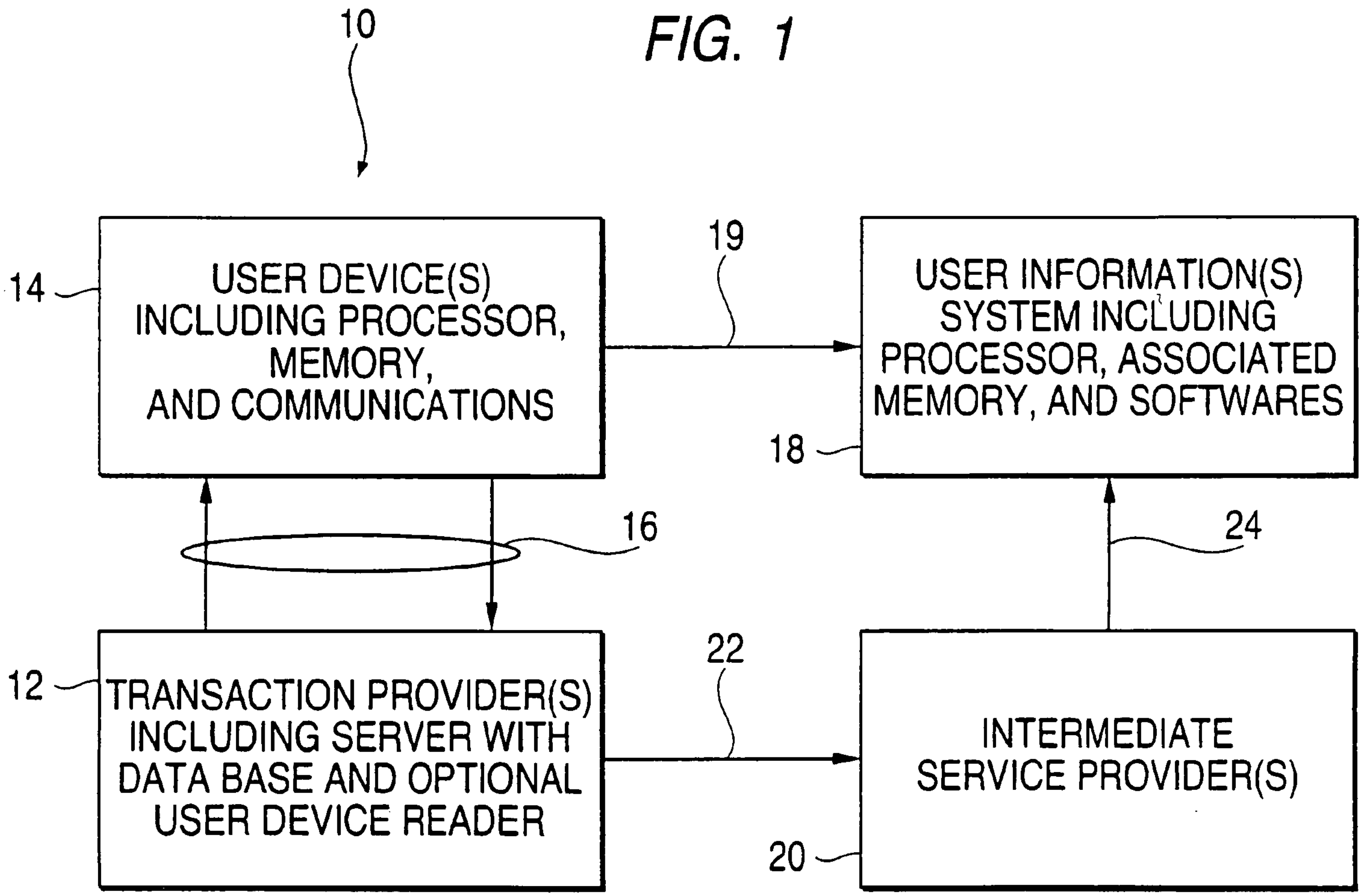

10
14
USER DEVICE(S)
INCLUDING PROCESSOR,
MEMORY,
AND COMMUNICATIONS
19
USER INFORMATION(S)
SYSTEM INCLUDING
PROCESSOR, ASSOCIATED
MEMORY, AND SOFTWARES
18
16
24
12
TRANSACTION PROVIDER(S)
INCLUDING SERVER WITH
DATA BASE AND OPTIONAL
USER DEVICE READER
22
INTERMEDIATE
SERVICE PROVIDER(S)
20

FIG. 2

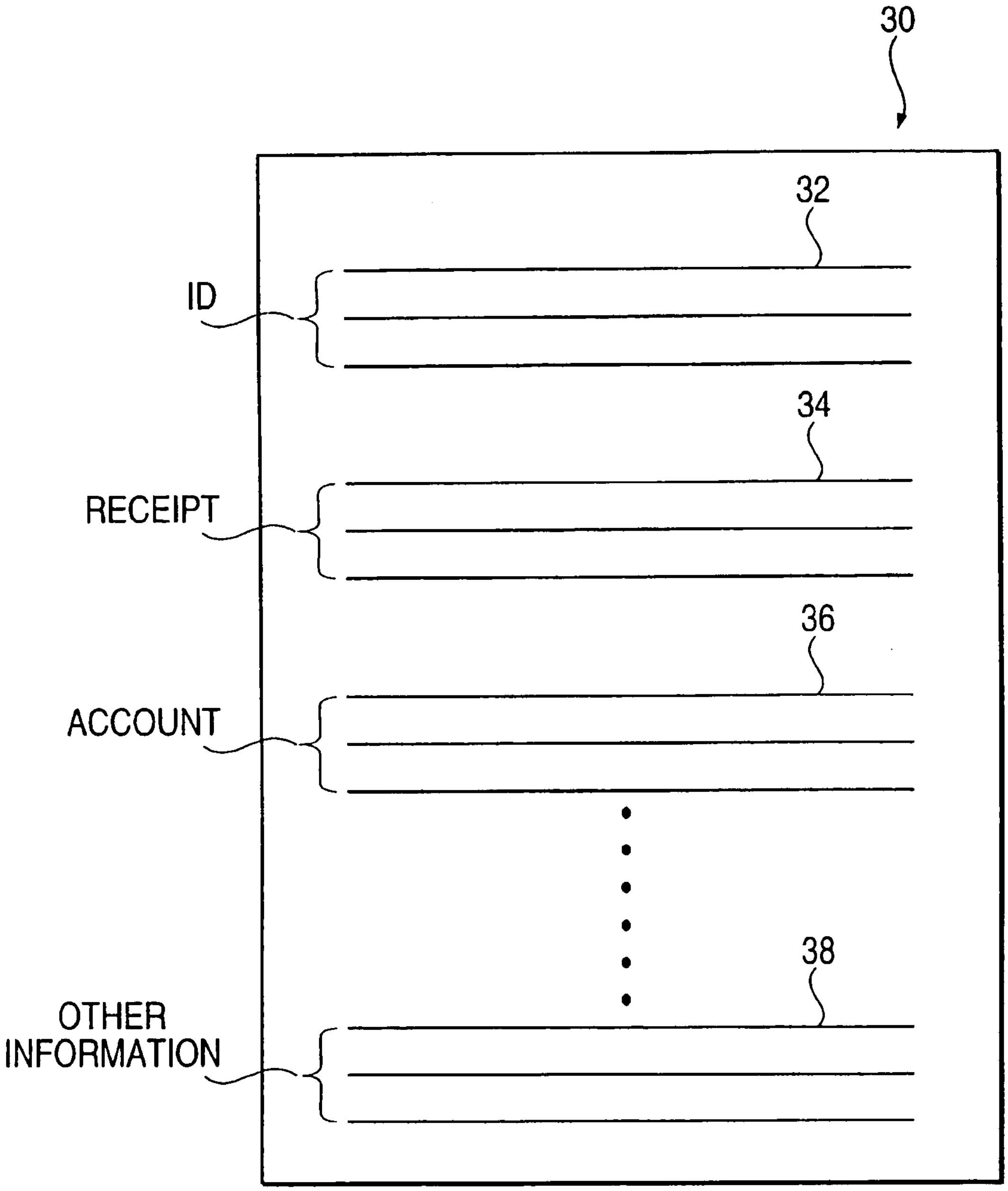


FIG. 3A

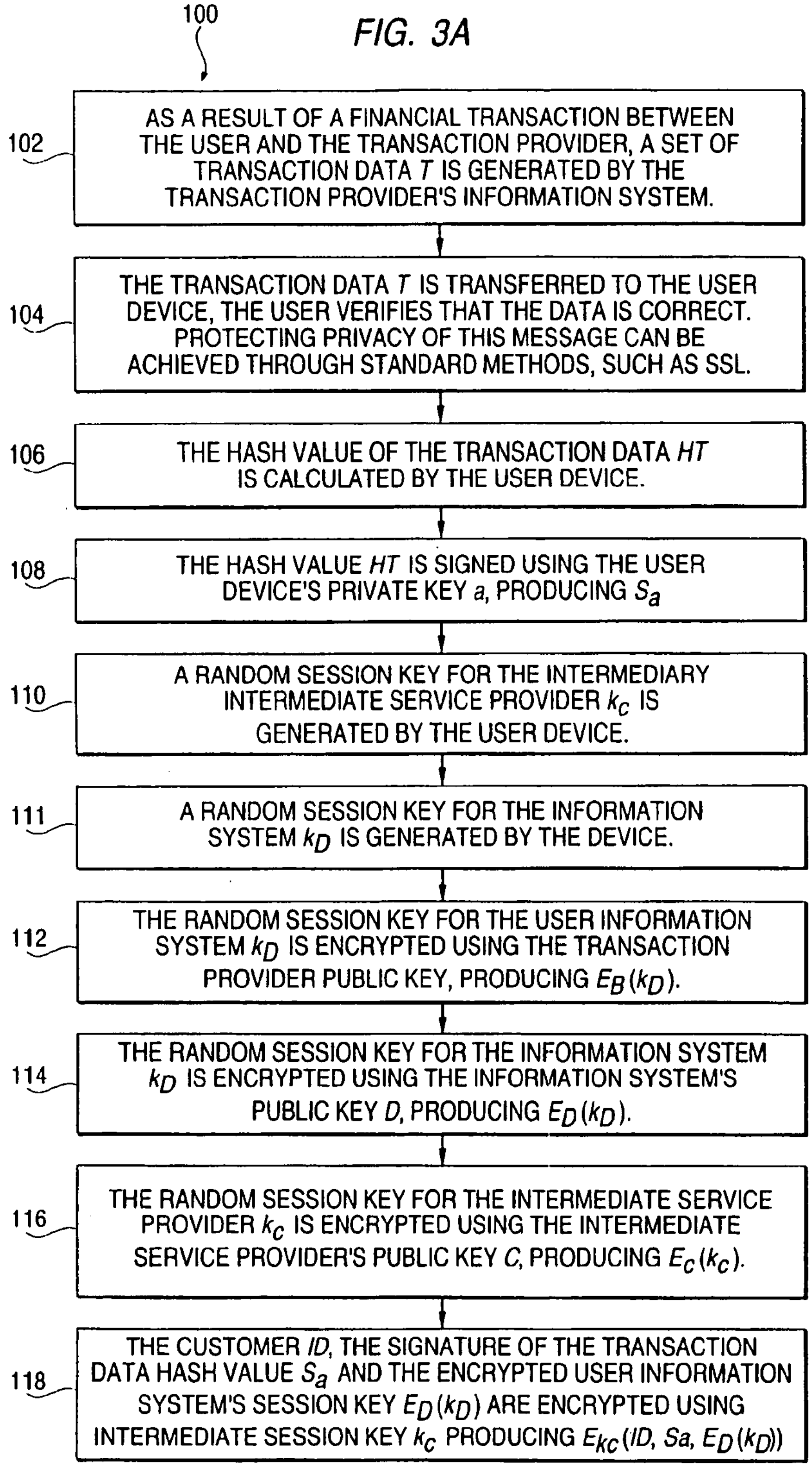
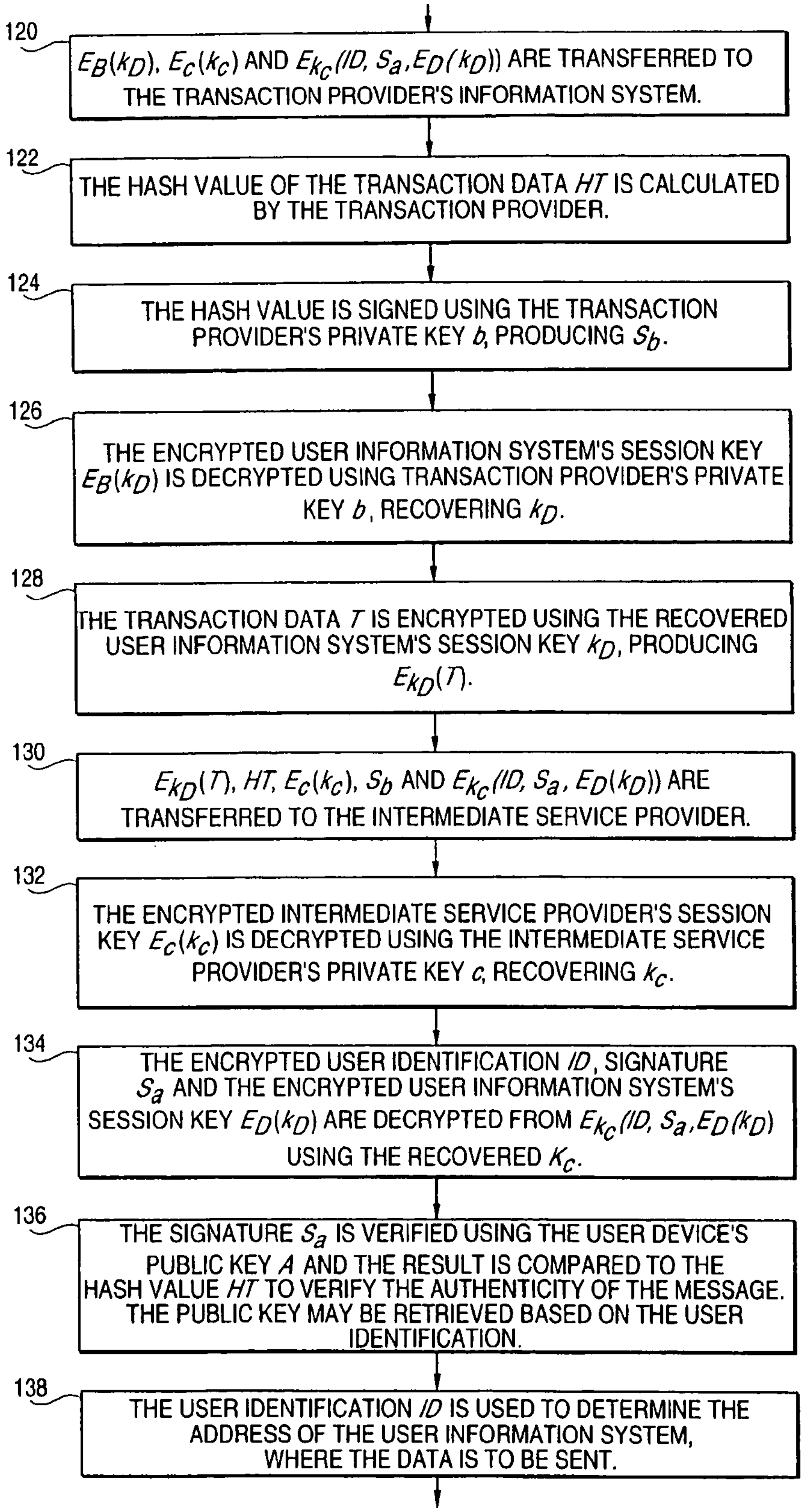

100
102
AS A RESULT OF A FINANCIAL TRANSACTION BETWEEN THE USER AND THE TRANSACTION PROVIDER, A SET OF TRANSACTION DATA *T* IS GENERATED BY THE TRANSACTION PROVIDER'S INFORMATION SYSTEM.
104
THE TRANSACTION DATA *T* IS TRANSFERRED TO THE USER DEVICE, THE USER VERIFIES THAT THE DATA IS CORRECT. PROTECTING PRIVACY OF THIS MESSAGE CAN BE ACHIEVED THROUGH STANDARD METHODS, SUCH AS SSL.
106
THE HASH VALUE OF THE TRANSACTION DATA *HT* IS CALCULATED BY THE USER DEVICE.
108
THE HASH VALUE *HT* IS SIGNED USING THE USER DEVICE'S PRIVATE KEY *a*, PRODUCING S_a
110
A RANDOM SESSION KEY FOR THE INTERMEDIARY INTERMEDIATE SERVICE PROVIDER k_C IS GENERATED BY THE USER DEVICE.
111
A RANDOM SESSION KEY FOR THE INFORMATION SYSTEM k_D IS GENERATED BY THE DEVICE.
112
THE RANDOM SESSION KEY FOR THE USER INFORMATION SYSTEM k_D IS ENCRYPTED USING THE TRANSACTION PROVIDER PUBLIC KEY, PRODUCING $E_B(k_D)$.
114
THE RANDOM SESSION KEY FOR THE INFORMATION SYSTEM k_D IS ENCRYPTED USING THE INFORMATION SYSTEM'S PUBLIC KEY *D*, PRODUCING $E_D(k_D)$.
116
THE RANDOM SESSION KEY FOR THE INTERMEDIATE SERVICE PROVIDER k_C IS ENCRYPTED USING THE INTERMEDIATE SERVICE PROVIDER'S PUBLIC KEY *C*, PRODUCING $E_C(k_C)$.
118
THE CUSTOMER *ID*, THE SIGNATURE OF THE TRANSACTION DATA HASH VALUE S_a AND THE ENCRYPTED USER INFORMATION SYSTEM'S SESSION KEY $E_D(k_D)$ ARE ENCRYPTED USING INTERMEDIATE SESSION KEY k_C PRODUCING $E_{kC}(ID, Sa, E_D(k_D))$

FIG. 3B



120 $E_B(k_D)$, $E_C(k_C)$ AND $E_{k_C}(ID, S_a, E_D(k_D))$ ARE TRANSFERRED TO THE TRANSACTION PROVIDER'S INFORMATION SYSTEM.

122 THE HASH VALUE OF THE TRANSACTION DATA HT IS CALCULATED BY THE TRANSACTION PROVIDER.

124 THE HASH VALUE IS SIGNED USING THE TRANSACTION PROVIDER'S PRIVATE KEY b, PRODUCING S_b.

126 THE ENCRYPTED USER INFORMATION SYSTEM'S SESSION KEY $E_B(k_D)$ IS DECRYPTED USING TRANSACTION PROVIDER'S PRIVATE KEY b, RECOVERING k_D.

128 THE TRANSACTION DATA T IS ENCRYPTED USING THE RECOVERED USER INFORMATION SYSTEM'S SESSION KEY k_D, PRODUCING $E_{k_D}(T)$.

130 $E_{k_D}(T)$, HT, $E_C(k_C)$, S_b AND $E_{k_C}(ID, S_a, E_D(k_D))$ ARE TRANSFERRED TO THE INTERMEDIATE SERVICE PROVIDER.

132 THE ENCRYPTED INTERMEDIATE SERVICE PROVIDER'S SESSION KEY $E_C(k_C)$ IS DECRYPTED USING THE INTERMEDIATE SERVICE PROVIDER'S PRIVATE KEY c, RECOVERING k_C.

134 THE ENCRYPTED USER IDENTIFICATION ID, SIGNATURE S_a AND THE ENCRYPTED USER INFORMATION SYSTEM'S SESSION KEY $E_D(k_D)$ ARE DECRYPTED FROM $E_{k_C}(ID, S_a, E_D(k_D)$ USING THE RECOVERED K_C.

136 THE SIGNATURE S_a IS VERIFIED USING THE USER DEVICE'S PUBLIC KEY A AND THE RESULT IS COMPARED TO THE HASH VALUE HT TO VERIFY THE AUTHENTICITY OF THE MESSAGE. THE PUBLIC KEY MAY BE RETRIEVED BASED ON THE USER IDENTIFICATION.

138 THE USER IDENTIFICATION ID IS USED TO DETERMINE THE ADDRESS OF THE USER INFORMATION SYSTEM, WHERE THE DATA IS TO BE SENT.

FIG. 3C

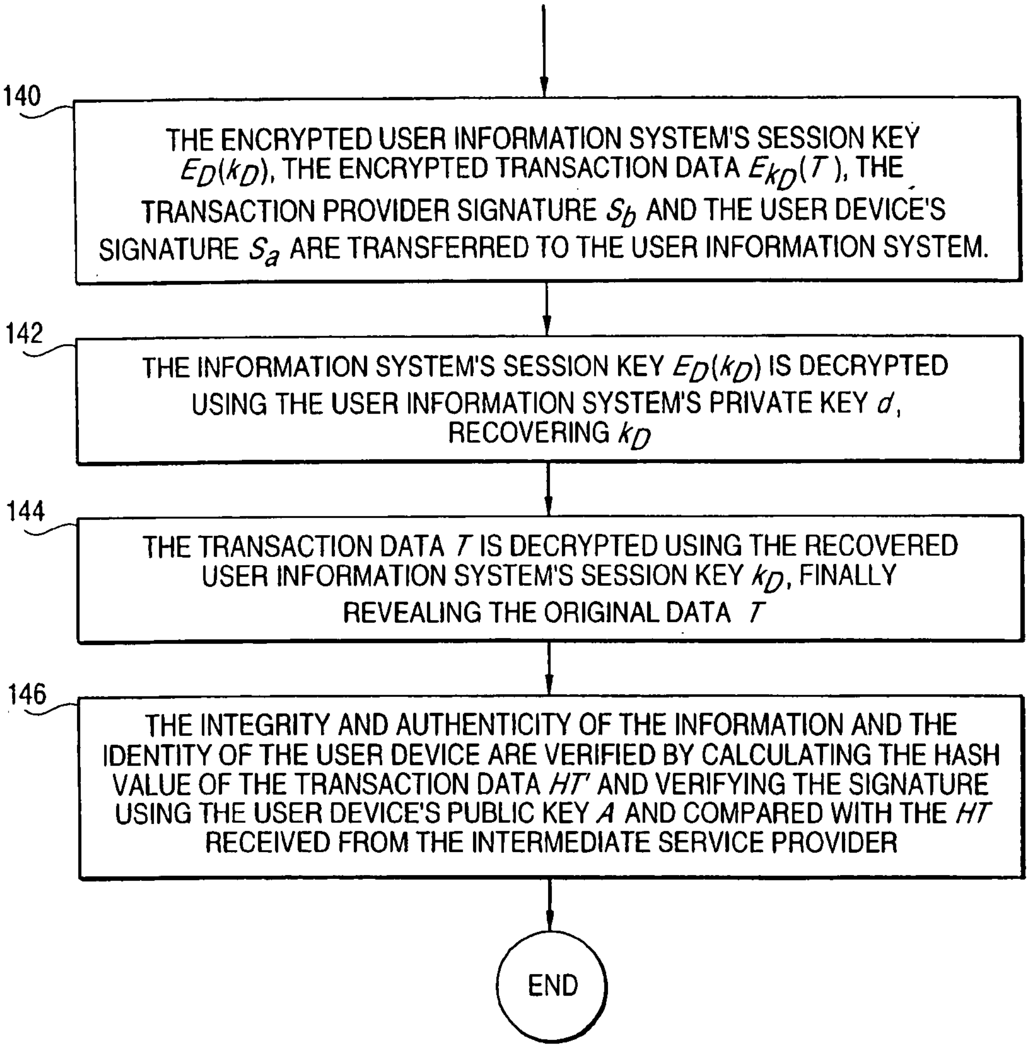

140
THE ENCRYPTED USER INFORMATION SYSTEM'S SESSION KEY $E_D(k_D)$, THE ENCRYPTED TRANSACTION DATA $E_{k_D}(T)$, THE TRANSACTION PROVIDER SIGNATURE S_b AND THE USER DEVICE'S SIGNATURE S_a ARE TRANSFERRED TO THE USER INFORMATION SYSTEM.
142
THE INFORMATION SYSTEM'S SESSION KEY $E_D(k_D)$ IS DECRYPTED USING THE USER INFORMATION SYSTEM'S PRIVATE KEY d, RECOVERING k_D
144
THE TRANSACTION DATA T IS DECRYPTED USING THE RECOVERED USER INFORMATION SYSTEM'S SESSION KEY k_D, FINALLY REVEALING THE ORIGINAL DATA T
146
THE INTEGRITY AND AUTHENTICITY OF THE INFORMATION AND THE IDENTITY OF THE USER DEVICE ARE VERIFIED BY CALCULATING THE HASH VALUE OF THE TRANSACTION DATA HT' AND VERIFYING THE SIGNATURE USING THE USER DEVICE'S PUBLIC KEY A AND COMPARED WITH THE HT RECEIVED FROM THE INTERMEDIATE SERVICE PROVIDER
END

FIG. 4A

USER DEVICE A

INPUT:

T

PROCESSING:

$HT = H(T)$,

$S_a = S_a(HT)$,

k_C,

k_D,

$E_B(k_D)$,

$E_D(k_D)$,

$E_{k_C}(ID, S_a, E_D(k_D))$,

OUTPUT:

$E_B(k_D)$,

$E_C(k_C)$,

$E_{k_C}(ID, S_a, E_D(k_D))$

FIG. 4B

TRANSACTION PROVIDER B
INPUT: T, $E_B(k_D)$, $E_C(k_C)$, $E_{k_C}(ID, S_a, E_D(k_D))$
PROCESSING: $HT = H(T)$, $S_b = S_b(HT)$, $k_D = D_b(E_B(k_D))$, $E_{k_D}(T)$
OUTPUT: $E_{k_D}(T)$, HT, S_b, $E_C(k_C)$, $E_{k_C}(ID, S_a, E_D(K_D))$

FIG. 4C

INTERMEDIATE SERVICE PROVIDER C

INPUT:

$E_{k_D}(T)$,

HT,

S_b,

$E_C(k_C)$,

$E_{k_C}(ID, S_a, E_D(k_D))$

PROCESSING:

$k_C = D_C(E_C(k_C))$,

$ID, S_a, E_D(k_D) = D_{k_C}(E_{k_C}(ID, S_a, E_D(k_D)))$

$HT' = V_A(S_a)$

OUTPUT:

$E_D(k_D)$,

$E_{k_D}(T)$,

S_a

FIG. 4D

USER INFORMATION SYSTEM D

INPUT:

$E_D(k_D)$,

$E_{k_D}(T)$,

S_a,

S_b

PROCESSING:

$k_D = D_d(E_D(k_D))$,

$T = D_{k_D}(E_{k_D}(T))$,

$HT = H(T)$,

$HT' = V_A(S_a)$

SYSTEM AND METHOD FOR COLLECTING FINANCIAL TRANSACTION DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and methods for gathering financial transaction data.

2. Description of the Prior Art

Point of sale systems are in widespread use at which a purchaser of goods or services pays with cash or a smart, credit or debit card. Transactions involving cards focus upon obtaining authorization from the credit or debit financial institution from which the purchaser is extended credit or at which a debit account is maintained and do not provide the purchaser with a detailed analysis of purchases beyond the minimum amount of information to permit the identification of the financial transaction. The information in billing statements regarding the purchased goods or services is not the equivalent of the receipt obtained at the point of sale by the purchaser. Furthermore, the monthly statement provided from the credit or debit organization contains insufficient information to be a useful tool for business and personal accounting and financial management.

The large body of information which is contained in the paperwork or otherwise associated with financial transactions generated by a point of sale or a business providing financial transactions on the internet or otherwise is not readily available electronically to the consumer of financial services. Paper receipts are voluminous to maintain and the collection of meaningful financial information based on receipts is a time intensive task for individuals and companies.

U.S. Pat. No. 4,277,837 discloses a personal portable terminal for financial transactions which facilitates electronic commerce. A personal data and storage transfer card is used in association with a personal portable terminal for continually monitoring and recording individual financial records. Verification of transactions between the user of the personal portable terminal and the party providing the transaction is facilitated. Storage is provided in the personal portable terminal which may be read out at a later date by a bank for auditing fund transfer and statement printing purposes. However, the personal portable terminal does not operate in association with a user information system which stores verified information including electronic receipts.

SUMMARY OF THE INVENTION

The present invention is a system and method for collecting data pertaining to financial transactions provided by a transaction provider which may be any form of commercial establishment, such as a point of sale for the purchase of goods or services or an entity providing electronic commerce, such as the purchase of goods or services over an IP network. The information which is collected with the present invention is utilized for business and personal accounting and financial management. The collected information includes at least an electronic receipt of the financial transaction but may also contain additional information which is stored by a user information system for facilitating business and personal accounting and financial management functions to the user. The user device communicates with the transaction provider selections of financial transactions made by the user of the user device which are offered by the user provider and information permitting the transaction provider to verify that the electronic receipt has been accepted by the user of the user device. The user information system communicates with at least one of the transaction provider or the user device and stores at least the electronic receipt which is received from the user device or the transaction provider which is verified by the user information system to have been accepted by the user of the user device. As a result of storage of at least the verified electronic receipt, the user information system becomes either a personal or business database which stores detailed information about the contents of the transaction and the individual items included in the transaction such as that which is typically recorded on a paper receipt.

The invention provides diverse benefits to users of the user device, transaction providers and intermediate service providers for developing business associated with the financial transaction. Examples are: customer buying information management, product buying information management, customer profile management, loyalty management, user information marketing, personal financial management, professional financial management and price tracking as described below.

The user information system eliminates the laborious process of collecting financial information from analysis of paper receipts. The information, including the electronic receipt which is stored by the user information system after verification, is a complete description of the financial transaction and is unlike the limited summary of information provided with a smart, credit or debit card billing statement. Instead of what amounts to a summary of each purchase which is included in a monthly statement of a smart, credit or debit card which is centered upon only the total amount of the purchase, the present invention collects substantial information about the details of each financial transaction, including an electronic receipt, any involved intermediate service provider, such as a bank or other financial institution from which smart, credit or debit services were obtained, including the identification of any accounts used for the financial transactions, the location from which the goods or services was purchased and the individual who entered into a financial transaction in a situation in which the user information system is providing storage of organizational information.

The information stored by the user information system records communications between a user of the user device and the transaction provider. As part of a financial transaction agreed upon between a user of the user device and the transaction provider, information which is normally recorded on a paper receipt is transmitted from an information storage system associated with the transaction provider to the information system associated with the user device. The communication is typified by communications between a cash register at a point of sale and the user device which the user is carrying or electronic commerce involving transaction providers which use IP networks to offer their financial transactions. The user device may use diverse types of softwares, including without limitation a personal financial assistance program or a company's accounting or operation management system. The information relating to the financial transaction including the electronic receipt may contain information facilitating automatic processing of the collected information, such as universal product codes (bar codes) representative of the financial transactions. Additionally, a user of the user device may annotate the information which is collected pertaining to all financial transactions with additional comments or classifications either at the time of entry into the financial transaction or at a later time. The storing of the information by the user information system including the electronic receipt may be in any form which facilitates personal or business accounting requirements.

The communications between the user device and the user information system may be implemented in many ways. For example, communications between the transaction provider, such as a cash register located at a retail point of sale, and the user device may be based upon low power wireless communications such as, for example, the proposed Bluetooth standard or a physical interface, such as when the user device is a card, such as a smartcard, which is inserted into a smart card reader of the transaction provider to transmit data from the card to the transaction provider regarding selections or verifications of the financial transaction, e.g. an electronic signature. The user device may contain memory and communication capabilities which facilitate the storage by the user device of at least the electronic receipt which is stored by the user information system after verification. Alternatively, the user device may communicate directly with the user information system after a verification of the financial transaction between the user and the transaction provider via communication mediums such as cellular communications using short message service (SMS). The user device may be a mobile terminal including a telephone interface with a personal digital assistant (PDA). Alternatively, the user device may contain communication capability with a IP network, such as the internet, to enter into financial transactions with the transaction provider.

While in a preferred embodiment the user device contains communication capabilities and substantial memory, the present invention is not limited to the user device having either communication capability or memory for storing electronic receipts and other information. As an alternative, the user device may be a device such as, but not limited to, a smart card which provides only a digital signature of the user to the transaction provider, which enables the transaction provider to forward at least the user authorized electronic receipt and other information to the user information system optionally through an intermediate service provider. Forwarding of at least the electronic receipt to the user information system may be directly or through the aforementioned intermediate service provider, which processes information relating to the accepted financial transaction transmitted by the transaction provider to the intermediate service provider to produce processed information pertaining to the accepted financial transactions. The intermediate service provider may be, without limitation, a financial institution, such as a bank or a smart, credit or debit card clearinghouse, which processes the information relating to the selected financial transaction against an account which the user has with the intermediate service provider.

The generation of an electronic signature by the user device has two purposes. First, the signature prevents the transaction provider or another party from falsifying the electronic receipt and other information which has been accepted by the user of the user device and furthermore, provides the transaction provider, such as a merchant with authorization, to transmit at least the electronic purchase information to the intermediate service provider, such as the user's financial institution where the amount of the transaction is posted against the user's account. The user information system provides verification of the information received from the transaction provider and may accept only information that has been properly electronically signed. Utilization of the transaction provider's information system, instead of relying upon the user's device for transmitting at least the electronic receipt, provides a substantial benefit in simplifying the user's device. Simplification of the user's device eliminates a requirement for complex communication capacity and obtains the benefit of the existing communication infrastructure associated with at least the transaction provider and optionally the intermediate service provider to facilitate communications of at least the electronic receipt to the user's information system. The association of the electronic signature with the electronic receipt permits the transaction provider to verify acceptance of the financial transaction recorded in the electronic receipt. Additionally, the storage of at least the electronic receipt, after verification of acceptance by the user information system, permits central processing immediately by the user information system. A memory of the user device, including a memory in a smartcard, provides a log of financial transactions which can be compared at a later time with the information stored in the user information system to verify that the transaction information has actually been received.

In view of the complete nature of the information contained in an electronic receipt associated with ;a financial transaction and other optional information which is gathered by the user device, suitable forms of encryption may be utilized to protect the identity of the user device and any sensitive information which is being transmitted between the user device, user information system, optional intermediate service provider and the user information system. The user device may encrypt the identity of the user from at least the transaction provider and may also encrypt the contents of the electronic receipt from being accessed by the intermediate service provider. The intermediate service provider, which may be a financial institution, may also protect the purchaser's identify when the identity of the user is encrypted with transmissions between the user device and the transaction provider.

The processing and communication capabilities of the optional intermediate service provider may be utilized in place of providing substantial processing and communication capability in the user device. When the user device has limited computing and communication capability, such limited capability may be used for the review of the electronic receipt from the transaction provider and signing thereof to permit the transaction provider to verify the transaction has been accepted by the user and then utilize either the transaction provider's or the optional intermediate service provider's additional processing and communication capability to further process or transmit at least the electronic receipt in a protected (encrypted) format to the user information system where after verification it is stored.

A system for collecting transaction data in accordance with the invention includes a transaction provider which provides at least an electronic receipt of financial transactions offered by the transaction provider; a user device, in communication with the transaction provider, which provides to the transaction provider a selection by a user of the user device of a financial transaction offered by the transaction provider and in response to receipt of an electronic receipt an acceptance of the financial transaction recorded in the electronic receipt; and a user information system, coupled to at least one of the transaction provider or the user device, which stores at least electronic receipts which are received from the user device or the transaction provider which are verified by the user information system to have been accepted by the user of the user device. The user device may be a mobile terminal in wireless communication with at least the transaction provider, a personal digital assistant in wireless communication with at least the transaction provider, or a smart card which is read by a smart card reader at the transaction provider to obtain at least the selection by the user of the financial transaction and information permitting the transaction provider to verify that the electronic receipt is accepted by the user of the user device. The user device may add to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system information. The information provided by the user device to permit the transaction provider to verify that the electronic receipt is accepted may comprise an electronic signature. The user information system also may verify at least any received electronic receipts with the electronic signature. The user device may add to the electronic receipt comments from the user providing additional information about the financial transaction beyond information contained in an electronic receipt.

A system for collecting transaction data in accordance with the invention also includes a transaction provider which provides at least an electronic receipt of financial transactions obtained from the transaction provider; a user device, in communication with the transaction provider, which provides to the transaction provider a selection by a user of the user device of a financial transaction offered by the transaction provider and in response to receipt of an electronic receipt, an acceptance of the transaction recorded in the received electronic receipt; an intermediate service provider, coupled to the transaction provider, which processes information relating to the accepted financial transaction transmitted by the transaction provider to the intermediate service provider to produce processed information pertaining to the accepted financial transaction; and a user information system, coupled to the intermediate service provider, which stores at least electronic receipts which are received from the intermediate service provider which are verified by the user information system to have been accepted by the user of the user device. The intermediate service provider may be a financial institution which processes the information relating to the accepted financial transaction against an account which the user has with the intermediate service provider. The user device may add to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system. The information provided by the user device to permit the transaction provider to verify that the electronic receipt is accepted may comprise an electronic signature. The user information system may also verify at least any received electronic receipts with the electronic signature. The user device may encrypt an identity of the user from at least the transaction provider. The user device may also encrypt the contents of the electronic receipt from being accessed by the intermediate service provider. The financial institution may validate the information relating to the accepted financial transaction is associated with the account of the user.

A process for collecting transaction data in accordance with the invention includes providing from a transaction provider to a user device at least an electronic receipt of a financial transaction obtained by the user from the transaction provider; providing a verification from the user device to the transaction provider that at least the electronic receipt is accepted by a user of the user device; transmitting from either the transaction provider or the user device to a user information system at least the electronic receipt; and storing at least the electronic receipt with the user information system when at least the electronic receipt is verified to have been accepted by the user of the user device. The user device may add to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipt stored by the user information system. Information may be provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted by the user of the user device. The information system used to verify the acceptance of received electronic receipts by the user of the user device may be an electronic signature. The transaction provider may also provide to the user device electronic data identifying financial transactions which are offered by the transaction provider.

A process for collecting transaction data in accordance with the invention includes providing from a transaction provider to a user device at least an electronic receipt of a financial transaction obtained by the user from the transaction provider; providing a verification from the user device to the transaction provider that at least the electronic receipt is accepted by a user of the user device; transmitting information relating to the accepted financial transaction from the transaction provider to an intermediate service provider; processing the information relating to the accepted financial transaction by the intermediate service provider to produce processed information pertaining to the accepted financial transaction; and receiving at least the electronic receipt with a user information system from the intermediate service provider and storing at least the electronic receipt when at least the electronic receipt is verified by the user information system to have been accepted by the user of the user device. The intermediate service provider may be a financial institution which processes the information relating to the accepted financial transaction against an account which the user has with the intermediate service provider. The user device may add to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipt stored by the user information system. Information is provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted. The information may comprise an electronic signature. The user device may encrypt an identity of the user from at least the transaction provider. The financial institution may validate the information relating to the accepted financial transaction is associated with the account of the user. The financial institution may provide information to the user information system that the financial transaction has occurred between the user and transaction provider.

The transaction provider and the intermediate service provider perform the following functions: the intermediate service provider may provide the transaction provider with an analysis of financial transactions accepted by the user of the user device which may be a statistical analysis; the transaction provider may provide an analysis of sales of particular types of financial transactions to manufacturers of products which are involved with the sale which may involve at least one of location and time that the sales were made; the transaction provider may create profiles of a user of the user device based on types of purchases which are made; the transaction provider may provide a tabulation of purchases made by users of the user device which may be provided by the transaction provider to a manufacturer of products purchased with each financial transaction; the intermediate service provider may provide a history of a user financial transaction to another for a benefit of the user; the intermediate service provider may provide a user of the user device with an analysis of the users history of financial transactions which may identify types of financial transactions which the user has accepted and the analysis group products which are involved in financial transactions according to categories; the analysis may compare the user's history of financial transactions with a history of financial transactions of others; and the user device may be used by members of an organization and information of multiple users is combined in the user information system.

A system for collecting transaction data in accordance with the invention includes a plurality of transaction providers, each transaction provider providing at least an electronic receipt of financial transactions obtained therefrom; a plurality of user devices, in communication with the plurality of transaction providers, which provide to at least one transaction provider a selection by a user of each user device of a financial transaction offered each transaction provider and in response to receipt of an electronic receipt an acceptance of the transaction recorded in the received electronic receipt; at least one intermediate service provider, coupled to each transaction provider, which processes information relating to the accepted financial transaction transmitted by each transaction provider to the at least one intermediate service provider to produce processed information pertaining to the accepted financial transaction; and at least one user information system, coupled to at least one intermediate service provider, each user information system storing at least electronic receipts which are received from each intermediate service provider which are verified by the at least one user information system to have been accepted by the user of each user device. The intermediate service provider may provide to at least one user of the user devices information on price differences at different locations at which the plurality of transaction providers are located.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a block diagram of an embodiment of a system for collecting transaction data in accordance with the present invention.

FIG. 2 illustrates an example format of at least the electronic receipt which is stored by a user information system in accordance with the present invention.

FIGS. 3A–3C illustrate a flowchart of one embodiment of a process for collecting transaction data in accordance with the present invention.

FIGS. 4A–4D illustrate the inputs, processes and the outputs of the process of FIGS. 3A–3C.

Like reference numerals identify like parts throughout the drawings.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. 1 illustrates a block diagram of a system 10 for collecting transaction data in accordance with the invention. Financial transactions and financial data should be understood to describe without limitation any transaction which involves exchange of monetary or other value between the user(s) of at least one user device 14 and at least one transaction provider 12. The system 10 is comprised of at least one transaction provider 12, at least one user device 14 which communicates with the transaction provider 12 over either a physical connection, wireline or a wireless communication link 16, at least one user information system 18, which communicates with the user device 14 over a communication link 19, which may be wireless or wireline or through at least one intermediate service provider 20 which communicates directly with the transaction provider 12 over a communication link 22, which may be wireless or wireline, and directly by communication link 24 with the user information system which may be either a wireless or a wireline link. It should be understood that only a single translation provider 12, user device 14, user information system 18 and intermediate service provider 20, have been illustrated for the purpose of simplifying illustration of a system in accordance with the present invention but, in practice, the invention is practiced with plural transaction providers, user devices, user information systems and intermediate service providers and the necessary illustrated communication links 16, 20, 22 and 24.

The transaction provider 12 may be, without limitation, any entity which provides financial transactions, such as, but not limited to, a retail organization, any point of sale (POS) entity or an entity providing electronic commerce, such as entities operating on IP networks. The transaction provider 12 may include a server with a database which manages the generation of electronic receipts by the transaction provider in response to selection of financial transactions offered by the transaction provider 12 by the user of the user device 14 and further verification that the electronic receipt transmitted by the transaction provider 12 to the user device 14 has been accepted by the user device to be correct. The verification of acceptance of at least the electronic receipt by the transaction provider 12 may be an electronic signature generated by any known technique or mechanism and provides the legal basis for the transaction provider to signal the intermediate service provider 20 that the financial transaction has been accepted by the user of the user device. Without limitation, the intermediate service provider typically is a financial institution offering smart, credit or debit services to the user of the user device 14 which the user has authorized to be processed by the financial transaction against the user's account. The transaction provider 12 in a retail or other point of sale configuration typically contains a register for storing cash and smart, credit or debit card receipts and processing and communication capability for management of inventory, etc. and communication capability directly (not illustrated) with the user information system 18 or with the intermediate service provider 20. The transaction provider 12 may transmit substantial information over the communications link 16 to the user device 14 which advertises or otherwise communicates information about a wide range of financial transactions which are offered by the transaction provider in order to induce the user of the user device 14 1o enter into financial transactions with the transaction provider 12. The user device 14, may be diverse in nature and may be a smart card, a mobile terminal including a wireless, telephone or short range wireless communication link, such as the proposed Bluetooth specification, a PDA, etc. The user device 14 typically contains a processor and associated memory and the aforementioned communication capability providing communications over links 16 and 20.

The transaction provider 12 provides at least an electronic receipt of financial transactions offered, by the transaction provider to the user of the user device 14 but typically also provides electronic data transmissions identifying financial transactions which are offered by the transaction provider which is a mechanism to induce purchase by the user of the user device 14 of financial transactions offered by the transaction provider 12. The user device 14 communicates over communication link 16 with the transaction provider 12 a selection by the user of the user device of a financial transaction offered by the transaction provider. Additionally, information is provided by the user device 14 to the transaction provider 12, after receipt by the user device of the electronic receipt, permitting the transaction provider to verify that the electronic receipt is accepted by the user. This verification information may without limitation be an electronic signature or simply an acknowledgment that the information contained in an electronic receipt transmitted by the transaction provider 12 to the user device 14 is acknowledged by the user of the user device to be accepted as a binding transaction.

The user information system 18 includes a processor and associated memory which stores at least electronic receipts which are received from the user device via direct communications over communication link 19 or, alternatively, by communication from the user device 14 over communication link 16 to the transaction provider 12, from the transaction provider 12 over communication link 22 to the intermediate service provider 20 and from the intermediate service provider 20 over communication link 24 to the user information system or directly from the transaction provider 22 such as when the intermediate service provider 20 is not present or is not operative. The user information system 18 includes softwares which process; at least the electronic receipt to permit verification as accepted by the user of the user device before storage in the memory. If the user information system 18 is an organization's system, such as a company, the processor may be in a server or part of a network of computers of the organization. The softwares may be diverse in nature and may include without limitation programs for accounting and financial management of the user of the user device 14 and decrypting of information as described below in FIGS. 3A–3C. These softwares provide a basis for decision making and maintaining personal or company budgets to provide prudent financial management and furthermore, facilitate the collection of transaction information in electronic form in the same manner in which the information was created by the transaction provider 12 as accepted by the user of the user device 14.

A preferred form of verification utilizes an electronic signature generated by the user of the user device 14. The electronic signature, generated by any known technique, which is transmitted by the user device 14 to the transaction provider 12 in response to receipt of at least an electronic receipt from the transaction provider, permits the transaction provider to authorize the intermediate service provider 20 to post the financial transaction against the smart, credit or debit account of the user of the user device 14 maintained by the intermediate service provider 20 which may be a bank or other financial institution. In addition to the approval of the electronic receipt and the financial transaction, additional information may be associated with the financial transaction by the user of the user device which is used by the user information system 18 in processing at least the electronic receipt stored by the user information system memory. Such additional information may be comments or personal annotations provided by the user of the user device 14 or information to be used during a processing of at least the electronic receipt by the user information system including software, etc. The electronic signature which is added by the user of the user device 14 to the electronic receipt prevents the transaction provider or a third party from falsifying the information of the accepted electronic receipt end further provides a preferred basis for the user information system 18 to verify that information transmitted thereto is information accepted by the user of the user device which should be stored in the memory in the user information system.

In view of the sensitivity of the substantial quantity of information which may be generated by the transaction provider 12 in the electronic receipt and further personal information which the user of the user device 14 may wish to annotate or otherwise associate with the electronic receipt in confidential form which is safeguarded from being disclosed or available to unauthorized individuals, it is possible to conceal the user's identity from the transaction provider and details of the financial transaction other than those necessary to perform smart, credit or debiting services on behalf of the user of the user device 14 by the intermediate service provider 20. This concealment may be accomplished by any known encrypted/decryption processes.

FIG. 2 illustrates an example of user information 30 which is stored in the memory of the user information system 18 including an electronic receipt 34. It should be understood that the user information 30 is only exemplary of possible types of information which may be stored and the form of storage of information stored by the user information system 18. The user information 30 includes identification information 32 of the user device 14 which may be of any diverse type, such as a social security number or other individual identification issued by countries of the user, company, etc., an electronic receipt 34, account information 36, and other information 38. The identification information 32 is utilized in the process described below in conjunction with FIGS. 3A–3C and FIGS. 4A–4D at least to obtain the address of the user identification information system 18 to which information is transmitted by the intermediate service provider 20 but may have other functions. The electronic receipt 34 may contain a whole host of identifying information regarding the financial transaction, such as, but not limited to, the information which is provided on a paper receipt but also including additional information such as product attributes, quantity, manufacturers's identity, EAN codes, such as a UPC code, which may be stored in any agreed upon format. The electronic receipt 34 is information which in the prior art was not provided by the billing statements from intermediate service providers 20 to the user in a normal smart, credit or debit card statement provided on a monthly basis and is the information which is highly useful in the user's accounting and/or financial management functions and further, to the transaction provider 12, the user of the user device 14 and the intermediate service provider 20 as a source of beneficial or saleable information as described below. The account information 36 is the customary information, such as a smart, credit or debit account number or other identification of services provided by the intermediate service provider 20. Finally, the other information 38 is symbolic of diverse forms of information which the user of the user device 14 wishes to store in the memory of the user information system 18 or otherwise use during the processing of information received by the user information system prior to storage in the memory and may without limitation include comments provided by the user of the user device 14 which annotate the particular financial transaction represented by the user information 30 and any softwares used to support storage or processing of the user information. The other information 38 may also be the source of information sold by the transaction provider 12 and/or the intermediate service provider 20 to the third parties as described below. It should be understood that the user information system 18 may be a company financial information system implemented in a server, an individual's home PC or otherwise.

The transaction provider 12 and the intermediate service provider 20 have a number of attractive possibilities for developing a business around the financial transaction information generated between the transaction provider and the user device 14. The categories of information are as follows:

1. CUSTOMER BUYING INFORMATION MANAGEMENT

Most importantly, if the customer identity is hidden by encryption or otherwise from the transaction provider **12**, the transaction provider has no way of identifying repeated purchases by the same customer. The intermediate service provider **20** may provide transaction providers **12** with statistical analysis of their customer's buying habits, or if allowed by the user, even the complete anonymous buying histories of single users. Additionally, if one transaction provider **12** serves multiple transaction provider locations of the same type, for example grocery stores, the transaction provider **12** may provide information on how the buying patterns of the customers of one store are different from buying patterns in other stores or buying patterns in general. This may take place, again, without revealing information of any other individual store.

2. PRODUCT BUYING INFORMATION MANAGEMENT

The same kind of analysis as consumer buying information is also possible on the product level. The transaction provider **12** may give product manufacturers information about how the sales of the product vary in different locations and at different times. Also, the buying histories of customers who have purchased the product can be compared to those who have not done so, or to those who have bought a competing product. This information can be used to analyze the segmentation of the market, for example to find that product A is favored over product B by heavy users. Buying of certain products together (e.g. refreshments) can also be analyzed.

3. CUSTOMER PROFILE MANAGEMENT

The transaction provider **12** can create profiles of customers based on their buying behavior. This information may be sold to third parties in an anonymous format and linked to other analysis.

4. LOYALTY MANAGEMENT

The transaction provider **12** can act as a loyalty scheme manager for transaction providers, or for product manufacturers. The transaction provider can prove for the transaction provider, that a certain number of purchases have been made by a certain user that gives the customer the right to receive some benefit (or that any other condition is fulfilled). If the user wishes, the user may reveal its identity to the transaction provider **12** in exchange for the benefit.

On the product buying level, the transaction provider **12** can accumulate purchases independent of the buying location (e.g. a certain grocery chain). For example, if a user buys Coca Cola® from different locations for a certain amount during a given period, the transaction provider may inform the user is eligible for a bonus CD from the Coca Cola Company.

5. USER INFORMATION MARKETING

More generally, the intermediary service provider **20** may market the information to third parties about the user's buying history in behalf of the user, who wants to receive money or other benefits in exchange. In this case, it is again essential that the user's identity can be protected from the transaction provider **12** by encryption or other techniques.

6. PERSONAL FINANCIAL MANAGEMENT

The intermediate service provider **20** may provide the users with a service detailing their consumption habits and history. This kind of service can be provided over the web or by using standard data formats for personal financial management software (i.e. Quicken).

The service can both give detailed records of committed purchases to the user, but in addition, to group products to categories. This way the user can for example follow, how much money has been used for food, clothing, home, car, amusement and other major categories at different times.

This information can be connected to financial planning applications, to enable the user to plan and follow their consumption in detail. The intermediate service provider **20** may provide the user with such planning services as well.

The service can also compare the purchasing behavior of the user, or user's household, to other similar users to show how the behavior differs from the typical user with the same background and income level.

Additionally, the information of purchases can be linked to other sources of information. For example, the purchased food items can be mapped to corresponding nutritional information, to provide the user with an indication of the healthiness of his diet.

7. PROFESSIONAL FINANCIAL MANAGEMENT

When a financial management service is provided to a commercial company, the information from multiple users can be automatically combined. Moreover, the information of purchases is available in almost real time, which may be significant to a large travelling work force or multiple remote sites.

8. PRICE TRACKING

The intermediate service provider **20** may provide users with information on price differences in different locations. It may allow the user to search for the lowest price of a product in an area, or calculate price indexes for groups of products, such as groceries. Moreover, it can compare the prices of a user's buying history at different locations to suggest the one that would have been the most inexpensive for the user.

FIGS. **3A–3C** illustrate a preferred embodiment of a process for collecting transaction data in accordance with the present invention which uses available cryptographic methods involving random session keys encrypted using public key cryptology. The described embodiment includes a protocol which hides the user's identity from the transaction provider **12** and optionally, the intermediate service provider **20** when desirable. The intermediate service provider **20** validates the information pertaining to the financial transaction and the user's identity and only allows the validated information to be processed. The aforementioned encryption also protects against third party unauthorized access when information is being transmitted between the various parts of the system of FIG. **1**. The process for collecting transaction information further permits verification that all of the transactions which have take place are correctly reported to the user information system.

Prior to description of each of the steps in FIGS. 3A–3C, the following notations are defined as used in FIGS. 3A–3D and 4A–4D:

$E_k(M)$ Encryption of message M, using key k

$S_k(M)$ Signature of message M, using key k

$D_k(M)$ Decryption of message M, using key k

$V_k(M)$ Verfication of message M, using key k

H(M) A one-way hash value of a message M

k_p A randomly generated session key for party P

A The user device **14**

B The transaction provide **12**

C The intermediate service provider **20**

D The user information system **18**

T A message containing the transaction data

HT=H(T) Hash value of the transaction data

ID Customer identification

k_c A random session key for the intermediate service provider **20**

$E_{k_c}($) Encryption using the intermediate service provider's session key

k_D A random session key for the user information system **18**

$E_{k_p}($) Encryption using the user information system's session key

$E_B($) Encryption using the transaction provider's public key

$E_C()$ Encryption using the intermediate service provider's public key

$E_D($) Encryption using the user information system's public key

$D_b($) Decryption using the transaction provider's private key

$D_c()$ Decryption using the intermediate service provider's private key

$D_d($) Decryption using the user information system's private key

S_a=S_a(HT) Signature of the transaction data hash value generated by the user device **14**

S_b=S_b(HT) Signature of the transaction data hash value generated by the transaction provider

With reference to FIGS. 3A–3C, the process **100** starts at point **102** where a financial transaction has occurred between the user of the user device **14** and the transaction provider **12** which results in a set of transaction data T being generated by the transaction provider's information system. The process proceeds to step **104** where the transaction data T is transferred to the user device **14** and the user device verifies that the data is correct. Protection of privacy of this message can be achieved through standard methods such as SSL. Processing proceeds to step **106** where the hash value of the transaction data HT is calculated by the user device **14**. Processing proceeds to step **108** where the hash value HT is signed by the user using the user device's private key "a" producing the quantity S_a. Processing proceeds to step **110** where a random session key K_c for the intermediate service provider **20** is generated by the user device **14**. Processing proceeds to step **111** where a random session key k_D for the user information system is generated by the user device **14**. Processing proceeds to step **112** where the random session key k_D for the user information system **18** is encrypted using the transaction provider's public key, producing $E_B(k_D)$. Processing proceeds to step **114** where the random session key k_D for the user information system **18** is encrypted using the user information system's public key D, producing $E_D(k_D)$. Processing proceeds to step **116** where the random session key k_c for the intermediate service provider **20** is encrypted using the intermediate service provider's public key C, producing $E_C(k_C)$. Processing proceeds to step **118** where the customer identification ID, the signature of the transaction data hash value S_a and the encrypted user information system's session key $E_D(k_D)$ are encrypted using the intermediate service provider's session key k_C, producing E_{k_c}, ID, S_a, $E_D(k_D)$. Processing proceeds to step **120** where the quantities $E_B(k_D)$, $E_c(k_c)$ and E_{k_c}(ID, S_a, $E_B(k_D)$) are transferred to the transaction provider's information system. Processing proceeds to step **122** where the hash values of the transaction data HT is calculated by the transaction provider. Processing proceeds to step **124** where the hash value is signed using the transaction provider's private key "b" producing S_b. Processing proceeds to step **126** where the encrypted user's information system's session key $B_b(k_D)$ is decrypted using the transaction provider's private key "b", recovering k_D. Processing proceeds to step **128** where the transaction data T is encrypted using the recovered user information system's session key k_D, producing E_D(T). Processing proceeds to step **130** where the quantities; E_kD(T), HT, $E_c(k_C)$, S_b and E_kC(ID), S_a, $E_D(k_D)$) are transferred to the intermediate service provider **20**. Processing proceeds to step **132** where the encrypted intermediate service provider's session key $E_C(k_C)$ is decrypted using the intermediate service provider's private key "c", recovering k_C. Processing proceeds to step **134** where the encrypted user identification ID, signature S_a and the encrypted user information system's session key $E_D(k_D)$ are decrypted from E_{k_c}(ID), S_a, $E_D(k_D)$) using recovered k_c. Processing proceeds to step **136** where the signature S_a is verified using the user device's public key A and the result is compared to the hash value HT to verify the authenticity of the message. The public key may be retrieved based upon the customer identification. Processing proceeds to step **138** where the customer identification ID is used to determine the address of the user information system where the data is to be sent. Processing proceeds to step **140** where the encrypted user information system's session key $E_D(k_D)$, the encrypted transaction data E_kD(T), the transaction provider's signature S_b and the user device's signature S_a are transferred to the user information system **18**. Processing proceeds to step **142** where the user information system's session key $S_D(k_D)$ is decrypted using the user information system's private key "d", recovering k_D. Processing proceeds to step **144** where the transaction data T is decrypted using the recovered user identification system's session key k_D, finally revealing the original transaction data T. Processing proceeds to step **146** where the integrity and authenticity of the transaction data and the identity of the user device are verified by calculating the hash value of the transaction data HT' and verifying the signature using the user's public key A and compared with the HT received from the intermediate service provider **20** which is the end of the process.

FIGS. 4A–4D identify the inputs, processings and outputs respectively of the user device **14**, transaction provider **12**, intermediate service provider **20** and user information system **18** of the process of FIGS. 3A–3C. The letter identifications "A–D" are respectively used in the various subscripts contained in the inputs, processings and outputs of the process of FIGS. 3A–3C to respectively identify the transaction provider **12**, user device **14**, user information system **18**, and the intermediate service provider **20**.

Additionally, the intermediate service provider **20** may have the electronic receipt and additional information transmitted thereto from the transaction provider **12** in non-encrypted form in order to permit the intermediate service provider to achieve profits or otherwise make financial use of the information therein as described above. This may be achieved by transmitting the information from the transaction provider **12** to the intermediate service provider **20** using a hybrid encryption based upon the intermediate service provider's public key.

Furthermore, if the intermediate service provider stores both S_a which equals S_a(HT) and S_b equal S_b(HT), disputes may later be resolved by the intermediate service provider between the user of the user device **14** and the transaction provider **12**. If either the user of the user device **14** or the transaction provider **12** reveals the transaction data T, the intermediate service provider **20** may calculate if the quantity HT equals H(T) and then verify whether the information was authenticate using the corresponding public keys.

Similarly, the signature S_b may be transferred to the user device **14**, which encrypts the signature using the intermediate service provider's session key before sending it forward. A log of all transaction times and signatures is therefore retained in the user device 14. If the user information system 18 has not received all transactions stored in the log, the user's possession of the signature may be used to prove that a questioned transaction actually took place.

Additionally, the intermediate service provider 20 may return a receipt of the received information to the transaction provider 12 thereby noting that the information transmitted by the transaction provider to the intermediate service provider was received correctly.

Finally, a simple protocol may be used to detect the comments and other information produced by the customer which do not pertain to the more sensitive electronic receipt and other transaction data.

While the invention has been described in terms of its preferred embodiments, it should be understood that numerous modifications may be made thereto without departing from the spirit and scope of the invention as defined in the appended claims. It is intended that all such modifications fall within the scope of the appended claims.

What is claimed is:

1. A system for collecting transaction data comprising:

a transaction provider which provides at least an electronic receipt of financial transactions offered by the transaction provider;

a user device, in communication with the transaction provider, which provides to the transaction provider a selection by a user of the user device of a financial transaction offered by the transaction provider and the user device in response to receipt of an electronic receipt provides an acceptance of the financial transaction recorded in the received electronic receipt to the transaction provider; and

a user information system, coupled to at least one of the transaction provider or the user device, which stores at least electronic receipts which are received from the user device or the transaction provider which are verified by the user information system to have been accepted by the user of the user device.

2. A system in accordance with claim 1 wherein:

the user device is a mobile terminal in wireless communication with at least the transaction provider.

3. A system in accordance with claim 2 wherein:

the user device adds to the electronic receipts additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system.

4. A system in accordance with claim 1 wherein:

the user information system comprises a processor and a memory with the memory storing at least electronic receipts only after the verification of acceptance of the electronic receipts by the user; and

the processor provides at least one of accounting service and financial management service to the user.

5. A system in accordance with claim 4 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system.

6. A system in accordance with claim 4 wherein:

the user information system stores in the memory transaction information of the user, is operated by a company physically separated from the user and is connected to the user device by a wireless link.

7. A system in accordance with claim 1 wherein:

the user device is a smart card which is read by a smart card reader at the transaction provider to obtain at least the acceptance by the user of the financial transaction and the information permitting the transaction provider to verify that the electronic receipt is accepted by the user of the user device.

8. A system in accordance with claim 7 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system.

9. A system in accordance with claim 7 wherein:

the information provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted by the user of the user device comprises an electronic signature.

10. A system in accordance with claim 9 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

11. A system in accordance with claim 1 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system.

12. A system in accordance with claim 11 wherein:

the information provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted by the user of the user device comprises an electronic signature.

13. A system in accordance with claim 11 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

14. A system in accordance with claim 1 wherein:

the user device adds to the electronic receipt comments from the user providing additional information about the financial transaction beyond information contained in an electronic receipt.

15. A system in accordance with claim 1 wherein:

the information provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted by the user of the user device comprises an electronic signature.

16. A system in accordance with claim 10 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

17. A system in accordance with claim 1 wherein:

the transaction provider also provides to the user device electronic data identifying financial transactions which are offered by the transaction provider.

18. A system for collecting transaction data comprising:

a transaction provider which provides at least an electronic receipt of financial transactions obtained from the transaction provider;

a user device, in communication with the transaction provider, which provides to the transaction provider a selection by a user of the user device of a financial transaction offered by the transaction provider and the user device in response to receipt of an electronic receipt provides an acceptance of the financial transaction recorded in the received electronic receipt to the transaction provider;

an intermediate service provider, coupled to the transaction provider, which processes information relating to the accepted financial transaction transmitted by the transaction provider to the intermediate service provider to produce processed information pertaining to the accepted financial transaction; and

a user information system, coupled to the intermediate service provider, which stores at least electronic receipts which are received from the intermediate service provider which are verified by the user information system to have been accepted by the user of the user device.

19. A system in accordance with claim 18 wherein:

the intermediate service provider is a financial institution which processes the information relating to the accepted financial transaction against an account which the user has with the intermediate service provider.

20. A system in accordance with claim 19 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system.

21. A system in accordance with claim 20 wherein:

the information provided by the user device to permit the transaction provider to verify that the electronic receipt is correct comprises an electronic signature.

22. A system in accordance with claim 21 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

23. A system in accordance with claim 19 wherein:

the information provided by the user device to permit the transaction provider to verify that the electronic receipt is correct comprises an electronic signature.

24. A system in accordance with claim 23 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

25. A system in accordance with claim 19 wherein:

the user device encrypts an identity of the user from at least the transaction provider.

26. A system in accordance with claim 25 wherein:

the user device also encrypts contents of the electronic receipt from being accessed by the intermediate service provider.

27. A system in accordance with claim 19 wherein:

the financial institution validates the information relating to the selected financial transaction is correct as associated with the account of the user.

28. A system in accordance with claim 27 wherein:

the financial institution provides information to the user information system that the financial transaction has occurred between the user and transaction provider.

29. A system in accordance with claim 18 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipts stored by the user information system.

30. A system in accordance with claim 29 wherein:

the information provided by the user device to permit the transaction provider to verify that the electronic receipt is correct comprises an electronic signature.

31. A system in accordance with claim 30 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

32. A system in accordance with claim 29 wherein:

the user device encrypts an identity of the user from at least the transaction provider.

33. A system in accordance with claim 32 wherein:

the user device also encrypts contents of the electronic receipt from being accessed by the intermediate service provider.

34. A system in accordance with claim 18 wherein:

the information provided by the user device to permit the transaction provider to verify that the electronic receipt is correct comprises an electronic signature.

35. A system in accordance with claim 34 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

36. A system in accordance with claim 35 wherein:

the user device encrypts an identity of the user from at least the transaction provider.

37. A system in accordance with claim 36 wherein:

the user device also encrypts contents of the electronic receipt from being accessed by the intermediate service provider.

38. A system in accordance with claim 34 wherein:

the user device encrypts contents of the electronic receipt from at least the transaction provider.

39. A system in accordance with claim 38 wherein:

the user device also encrypts contents of the electronic receipt from being accessed by intermediate service provider.

40. A system in accordance with claim 18 wherein:

the user device encrypts an identity of the user from at least the transaction provider.

41. A system in accordance with claim 40 wherein:

the user device also encrypts contents of the electronic receipt from being accessed by the intermediate service provider.

42. A system in accordance with claim 18 wherein:

the user information system comprises a processor and a memory with the memory storing at least electronic receipts only after the verification of acceptance of the electronic receipts by the user; and

the processor provides at least one of accounting service and financial management service to the user.

43. A system in accordance with claim 18 wherein:

the user information system stores in the memory transaction information of the user, is operated by a company physically separated from the user and is connected to the user device by a wireless link.

44. A process for collecting transaction data comprising:

providing from a transaction provider to a user device at least an electronic receipt of a financial transaction obtained by the user from the transaction provider;

providing a verification from the user device to the transaction provider in the electronic receipt that the financial transaction is accepted by a user of the user device;

transmitting from either the transaction provider or the user device to a user information system at least the electronic receipt; and

storing at least the electronic receipt with the user information system when at least the electronic receipt is verified by the user information system to have been accepted by the user of the user device.

45. A process in accordance with claim 44 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipt stored by the user information system.

46. A process in accordance with claim 44 wherein:

the information provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted by the user of the user device comprises an electronic signature.

47. A process in accordance with claim 46 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

48. A process in accordance with claim 44 wherein:

the transaction provider also provides to the user device electronic data identifying financial transactions which are offered by the transaction provider.

49. A process in accordance with claim 44 wherein:

the user information system comprises a processor and a memory with the memory storing at least electronic receipts only after the verification of acceptance of the electronic receipts by the user; and

the processor provides at least one of accounting service and financial management service to the user.

50. A process for collecting transaction data comprising:

providing form a transaction provider to a user device at least an electronic receipt of a financial transaction obtained by the user from the transaction provider;

providing a verification from the user device to the transaction provider in the electronic receipt that the financial transaction is accepted by a user of the user device;

transmitting information relating to the accepted financial transaction from the transaction provider to an intermediate service provider;

processing the information relating to the accepted financial transaction with the intermediate service provider to produce processed information pertaining to the accepted financial transaction; and

receiving at least the electronic receipt with a user information system from the intermediate service provider and storing at least the electronic receipt when at least the electronic receipt is verified by the user information system to have been accepted by the user of the user device.

51. A process in accordance with claim 50 wherein:

the intermediate service provider is a financial institution which processes the information relating to the selected financial transaction against an account which the user has with the intermediate service provider.

52. A process in accordance with claim 50 wherein:

the user device adds to the electronic receipt additional information which is used by the user information system in processing at least the electronic receipt stored by the user information system.

53. A process in accordance with claim 50 wherein:

the information provided by the user device to the transaction provider to permit the transaction provider to verify that the electronic receipt is accepted by the user of the user device comprises an electronic signature.

54. A process in accordance with claim 53 wherein:

the user information system also verifies at least any received electronic receipts with the electronic signature.

55. A process in accordance with claim 50 wherein:

the user device encrypts an identity of the user from at least the transaction provider.

56. A process in accordance with claim 55 wherein:

the user device also encrypts the contents of the electronic receipt from being accessed by the intermediate service provider.

57. A process in accordance with claim 51 wherein:

the financial institution validates the information relating to the accepted financial transaction is correct as associated with the account of the user.

58. A process in accordance with claim 57 wherein:

the financial institution provides information to the user information system that the financial transaction has occurred between the user and transaction provider.

59. A process in accordance with claim 50 wherein:

the intermediate service provider provides the transaction provider with an analysis of financial transactions accepted by the user of the user device.

60. A process in accordance with claim 59 wherein:

the analysis is a statistical analysis.

61. A process in accordance with claim 50 wherein:

the transaction provider provides an analysis of sales of particular types of financial transactions to manufacturers of products which are involved with the sale.

62. A process in accordance with claim 61 wherein:

the analysis involves at least one of location and time that the sales were made.

63. A process in accordance with claim 50 wherein:

the transaction provider creates profiles of a user of the user device based on types of purchases which are made.

64. A process in accordance with claim 50 wherein:

the transaction provider provides a tabulation of purchases made by users of the user device.

65. A process in accordance with claim 64 wherein:

the tabulation is provided by the transaction provider to a manufacturer of products purchased with each financial transaction.

66. A process in accordance with claim 50 wherein:

the intermediate service provider provides the history of a user financial transaction to another for a benefit of the user.

67. A process in accordance with claim 50 wherein:

the intermediate service provider provides a user of the user device with an analysis of the user's history of financial transactions.

68. A process in accordance with claim 67 wherein:

the analysis identifies types of financial transactions which the user has accepted.

69. A process in accordance with claim 68 wherein:

the analysis groups products which are involved in financial transactions according to categories.

70. A process in accordance with claim 68 wherein:

the analysis compares the user's history of financial transactions with a history of financial transactions of others.

71. A process in accordance with claim 50 wherein:

the user device is used by members of an organization and information of multiple users is combined in the user information system.

72. A process in accordance with claim 50 wherein:

the user information system comprises a processor and a memory with the memory storing at least electronic receipts only after the verification of acceptance of the electronic receipts by the user; and

the processor provides at least one of accounting service and financial management service to the user.

73. A process in accordance with claim 72 wherein:

the user information system stores in the memory transaction information of the user, is operated by a company physically separated from the user and is connected to the user device by a wireless link.

74. A process in accordance with claim 50 wherein:

the user information system comprises a processor and a memory with the memory storing at least electronic receipts only after the verification of acceptance of the electronic receipts by the user; and

the processor provides at least one of accounting service and financial management service to the user.

75. A process in accordance with claim 74 wherein:

the user information system stores in the memory transaction information of the user, is operated by a company physically separated from the user and is connected to the user device by a wireless link.

76. A system for collecting transaction data comprising:

a plurality of transaction providers, each transaction provider providing at least an electronic receipt of financial transactions obtained therefrom;

a plurality of user devices, in communication with the plurality of transaction providers, which provide to at least one transaction provider a selection by a user of each user device of an offered financial transaction and in response to receipt of an electronic receipt an acceptance of the transaction recorded in the received electronic receipt;

at least one intermediate service provider, coupled to each transaction provider, which processes information relating to the accepted financial transaction transmitted by each transaction provider to the at least one intermediate service provider to produce processed information pertaining to the selected financial transaction; and

at least one user information system, coupled to at least one intermediate service provider, each user information system storing at least electronic receipts which are received from each intermediate service provider which are verified by the at least one user information system to have been accepted by the user of each user device.

77. A system in accordance with claim 76 wherein:

the intermediate service provider provides to at least one user of the user devices information on price differences at different locations at which the plurality of transaction providers are located.

78. A system in accordance with claim 76 wherein:

the user information system comprises a processor and a memory with the memory storing at least electronic receipts only after the verification of acceptance of the electronic receipts by the user; and

the processor provides at least one of accounting service and financial management service to the user.

79. A system in accordance with claim 78 wherein:

the user information system stores in the memory transaction information of the user, is operated by a company physically separated from the user and is connected to the user device by a wireless link.

* * * * *

US006327576B1

(12) **United States Patent**
Ogasawara

(10) **Patent No.: US 6,327,576 B1**
(45) **Date of Patent: Dec. 4, 2001**

(54) **SYSTEM AND METHOD FOR MANAGING EXPIRATION-DATED PRODUCTS UTILIZING AN ELECTRONIC RECEIPT**

(75) Inventor: **Nobuo Ogasawara**, Atsugi (JP)

(73) Assignee: **Fujitsu Limited**, Kanagawa (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/400,124**

(22) Filed: **Sep. 21, 1999**

(51) **Int. Cl.**^{7} **G60G 1/14**
(52) **U.S. Cl.** **705/22**
(58) **Field of Search** 705/2, 22

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,866,661	9/1989	de Prins	364/900
4,973,828	11/1990	Naruse et al.	235/380
5,448,044	9/1995	Price et al.	235/380
5,469,363	11/1995	Saliga	364/478
5,590,038	12/1996	Pitroda	395/241
5,739,512	4/1998	Tognazzini	235/380
5,821,513	10/1998	O'Hagan et al.	235/383
5,845,256	12/1998	Pescitelli et al.	705/4
5,953,234 *	9/1999	Singer et al.	364/478.02
6,003,006 *	12/1999	Colella et al.	705/2

FOREIGN PATENT DOCUMENTS

0 942 383 A1 9/1999 (EP) .

OTHER PUBLICATIONS

Electronic Times, "Clever Containers", Sep. 6, 1999, p31.*

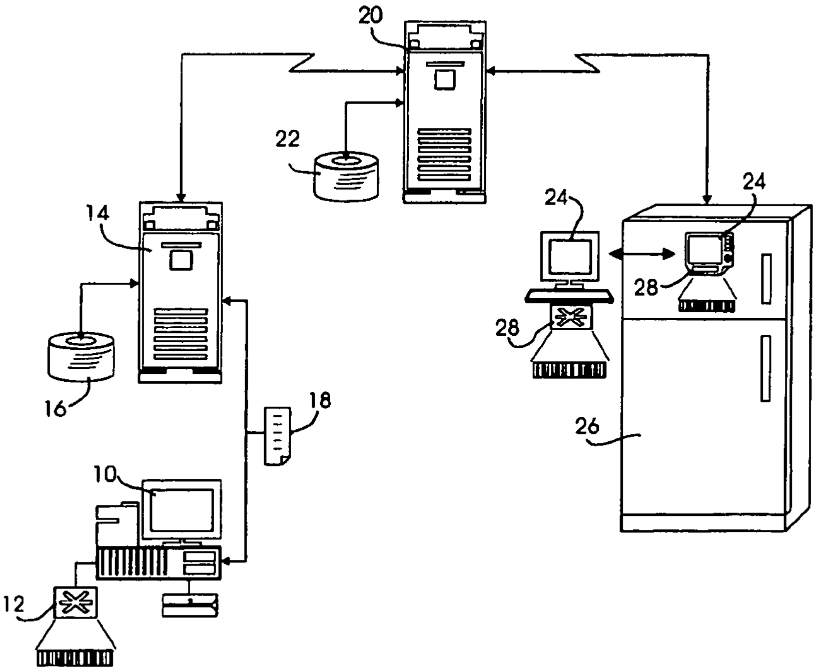
* cited by examiner

Primary Examiner—Kenneth R. Rice
(74) *Attorney, Agent, or Firm*—Christie, Parker & Hale, LLP

(57) **ABSTRACT**

The present invention provides apparatus, systems and methods by which information concerning the shelf-life limitations of a particular product item is made available to the purchaser electronically; that the electronically recorded shelf-life limitation information is provided to, or made accessible by, the purchaser; that the electronically recorded shelf-life limitation information is communicated to a computer equipped with a microprocessor, or to a computer system network, accessible by the purchaser, programmed to receive the shelf-life limitation data for each product for that purchaser; that the computer or purchaser-accessible computer system network, is further programmed to provide the purchaser with on-screen and/or printed reports of various formats that list the items purchased and the corresponding shelf-life limitation information; and that the computer or purchaser-accessible computer system network provides interactivity with the purchaser to allow the purchaser to identify further information to the computer/network, such as identifying location information of each particular product item, and the inventory status of each particular product item, e.g., whether the product has been opened or has been discarded.

10 Claims, 6 Drawing Sheets



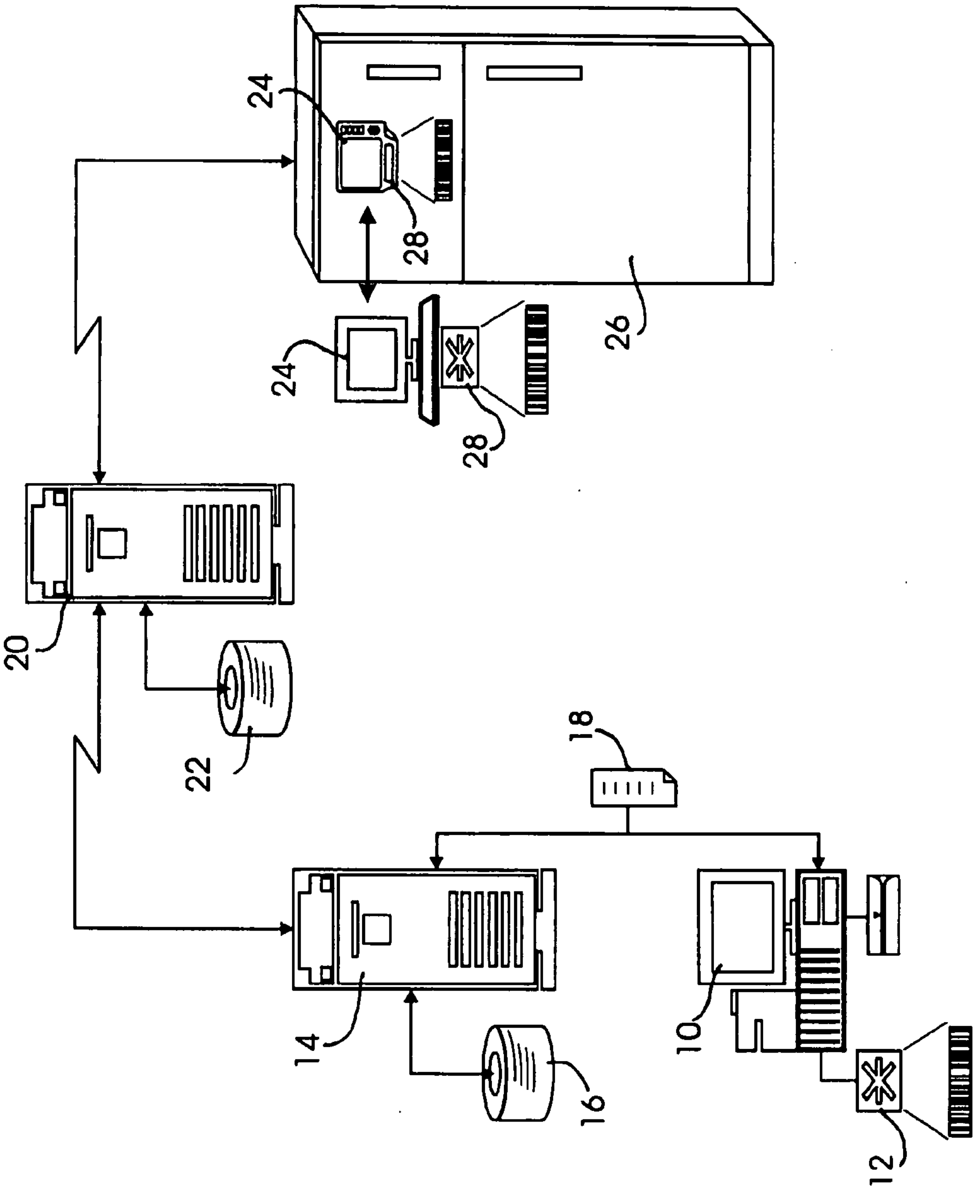


FIG. 1

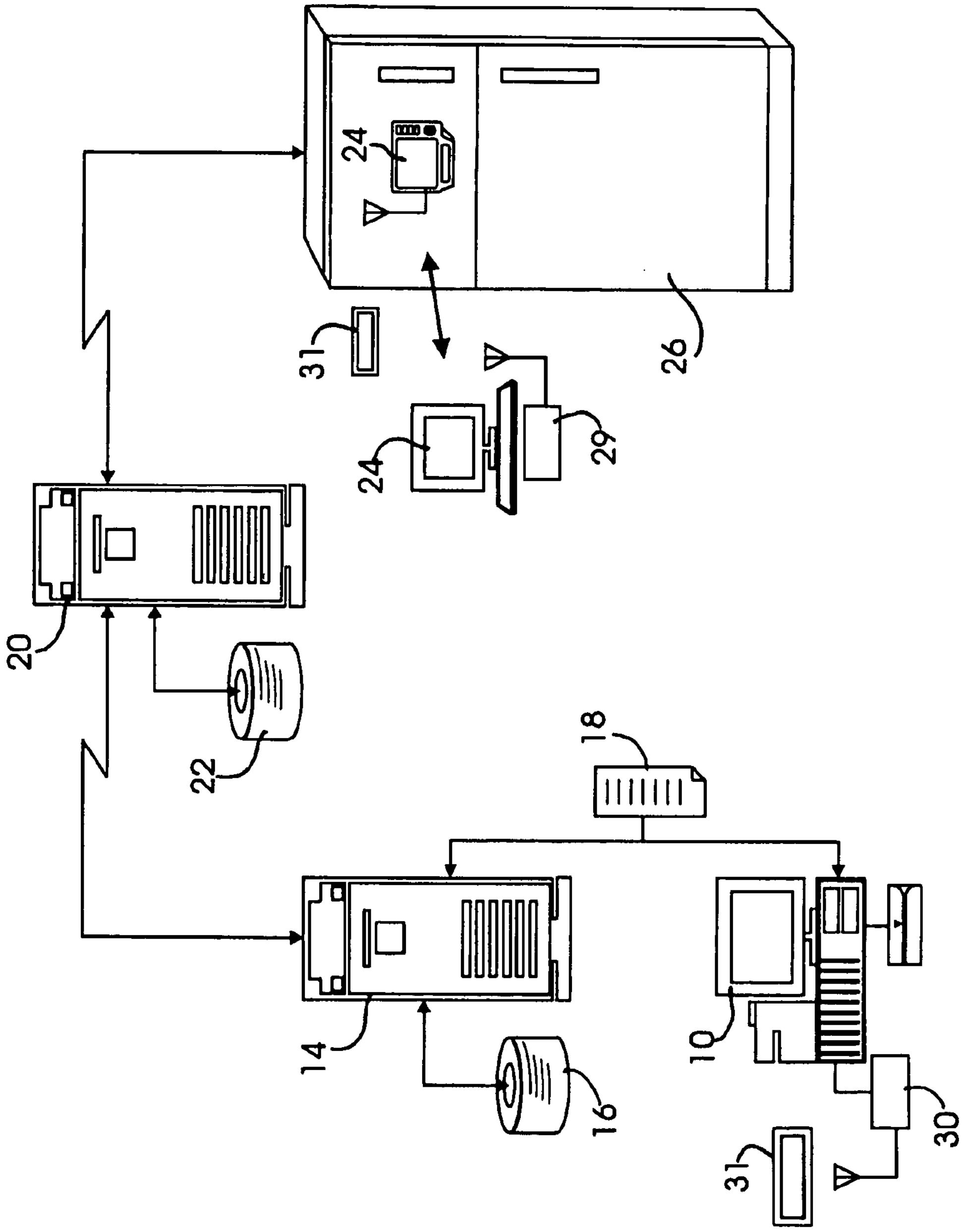


FIG. 2

Customer Name	Mike Smith				
Customer ID	123456				
Store Name	ABC Store, N.Y.				
Shopping Date and Time	01/01/98 11:30				
Item Description	Quantity	Price	UPC	Expiration Date	Freshness Period After Package Opened
Fuji Apples	6	6.98	41001111	01/15/98	
One gallon 2% low fat milk	2	7.48	41112222	01/07/98	
Country beef sausage	1	4.98	41223333	06/30/98	7 days
Low fat cream cheese	2	5.96	41334444	09/30/98	10 days
2-ply tissues	6	3.66	41445555		
Disney shampoo	1	3.48	41556666		
--------------------------	------	------	------	------	------
--------------------------	------	------	------	------	
TOTAL		58.66			

FIG. 4

UPC	Expiration Date	Freshness Period After Package Opened
41001111	01/15/98	
41112222	01/07/98	
41223333	06/30/98	7 days
41334444	09/30/98	10 days
41445555		
41556666		
------	------	------
------	------	

FIG. 3

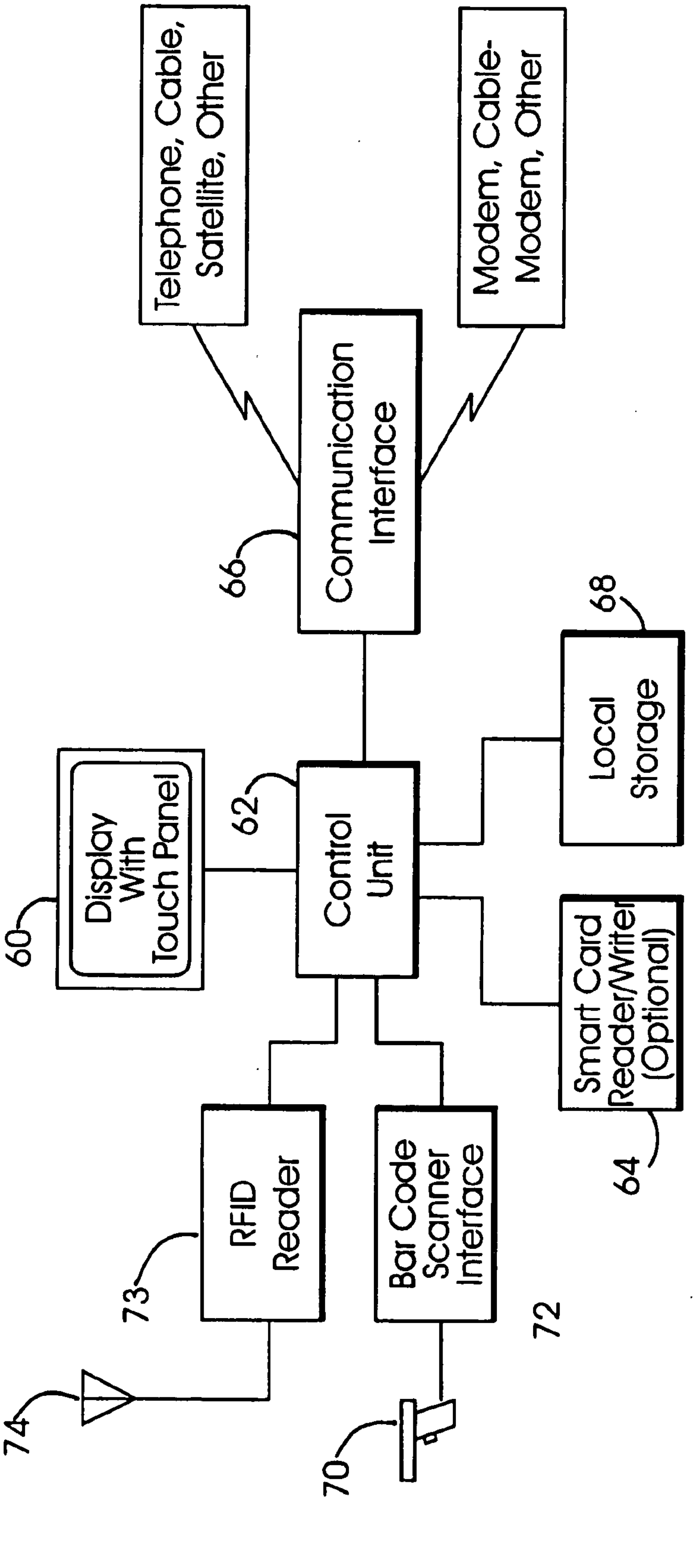
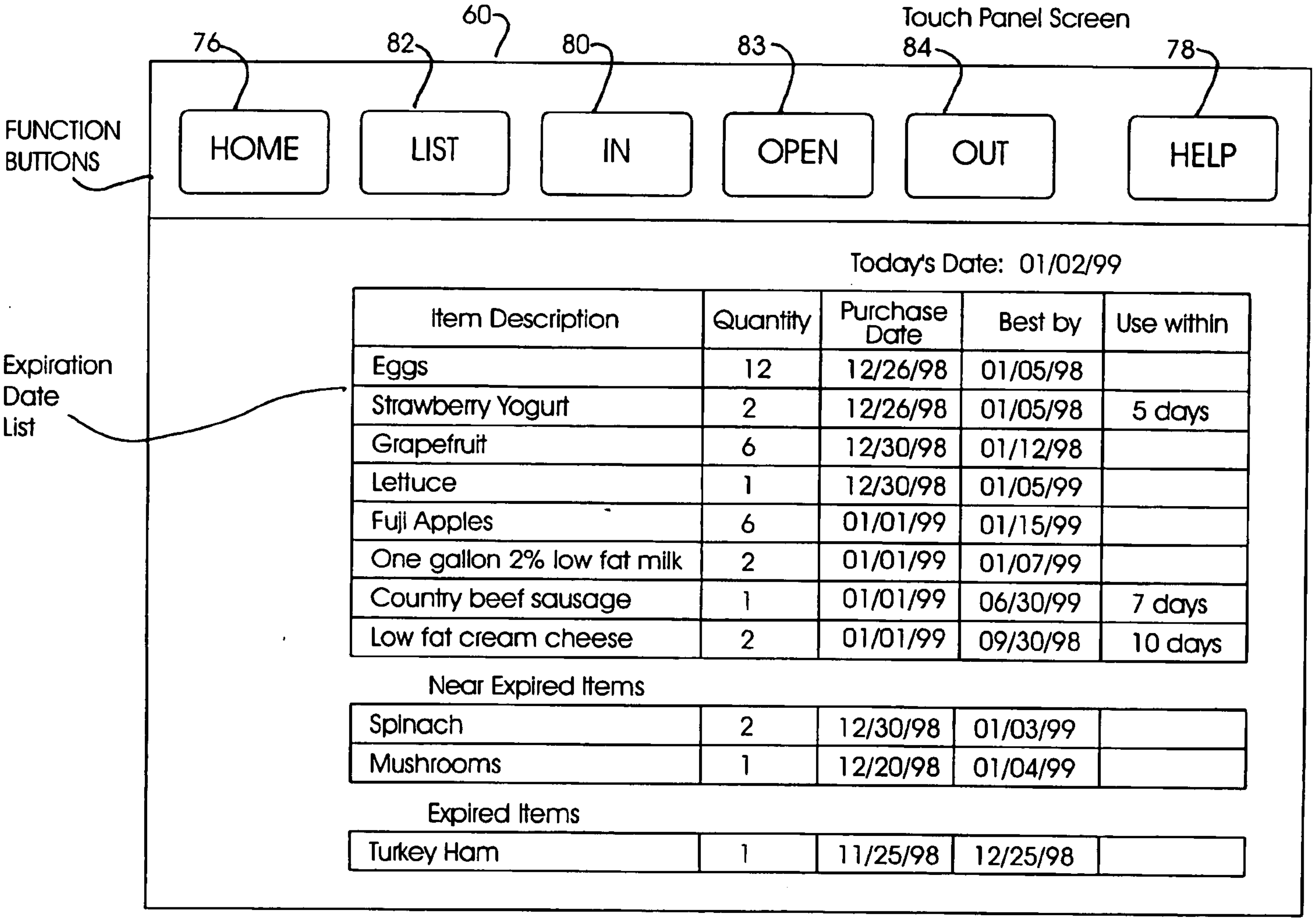

Telephone, Cable, Satellite, Other
Modem, Cable-Modem, Other
66
Communication Interface
68
Local Storage
60
Display With Touch Panel
62
Control Unit
Smart Card Reader/Writer (Optional)
64
73
RFID Reader
Bar Code Scanner Interface
72
74
70

FIG. 5

Today's Date: 01/02/99

Item Description	Quantity	Purchase Date	Best by	Use within
Eggs	12	12/26/98	01/05/98	
Strawberry Yogurt	2	12/26/98	01/05/98	5 days
Grapefruit	6	12/30/98	01/12/98	
Lettuce	1	12/30/98	01/05/99	
Fuji Apples	6	01/01/99	01/15/99	
One gallon 2% low fat milk	2	01/01/99	01/07/99	
Country beef sausage	1	01/01/99	06/30/99	7 days
Low fat cream cheese	2	01/01/99	09/30/98	10 days
Near Expired Items				
Spinach	2	12/30/98	01/03/99	
Mushrooms	1	12/20/98	01/04/99	
Expired Items				
Turkey Ham	1	11/25/98	12/25/98	

FIG. 6



Today's Date: 01/02/99

Item Description	Quantity	Purchase Date	Best by	Use within
Eggs	12	12/26/98	01/05/98	
Strawberry Yogurt	2	12/26/98	01/05/98	5 days
Grapefruit	6	12/30/98	01/12/98	
Lettuce	1	12/30/98	01/05/99	
Fuji Apples	6	01/01/99	01/15/99	
One gallon 2% low fat milk	2	01/01/99	01/07/99	
Country beef sausage	1	01/01/99	06/30/99	7 days
Low fat cream cheese	2	01/01/99	09/30/98	10 days

Near Expired Items

Spinach	2	12/30/98	01/03/99	
Mushrooms	1	12/20/98	01/04/99	

Expired Items

Turkey Ham	1	11/25/98	12/25/98	

FIG. 7

SYSTEM AND METHOD FOR MANAGING EXPIRATION-DATED PRODUCTS UTILIZING AN ELECTRONIC RECEIPT

FIELD OF THE INVENTION

The present invention relates generally to inventory control systems and methods and more particularly to apparatus, systems and methods for managing expiration-dated products.

BACKGROUND OF THE INVENTION

Many products and materials have a limited "shelf-life." That is, many products, ranging from pharmaceuticals to food products to batteries, are "fresh" for only a certain amount of time. In the case of pharmaceuticals, a particular compound may begin to lose its efficacy a certain amount of time after the compound is manufactured. In the case of unopened packaged food products, even the best packaging may allow deterioration of the freshness and/or quality of many food products a certain amount of time after the product is prepared and packaged. Even photographic film can only be trusted to preserve those precious moments for a certain amount of time after the film is manufactured and packaged. Once opened, many packaged products, such as food, deteriorate in freshness and/or quality within an abbreviated period of time.

Many products are labeled with an expiration date in a form readable by the purchaser. Some products are labeled with a "freshness period" that applies to the product once the packaging is opened (e.g., use within 48 hours of opening).

Typically, the purchaser of such limited shelf-life products must manually control the inventory of such products. Manual control is especially typical of residential and personal use products such as food, prescription medicines, photographic film and the like.

Typically, the approach used to expiration-date an item would be to calculate the expiration date based on the date on which the product is being manufactured; stamp the label of the product with the appropriate expiration date; apply the label to all product items of the specified type that are manufactured on that day. Since many of the containers used to store expiration dated products are manufactured well in advance of being filled with a perishable item, it is not presently feasible to expect an item's bar code to express expiration date information. Consequently, the expiration date information applied to each item is printed or stamped on the item's packaging only when the products are ready to ship. For example, milk and yogurt are packaged in containers pre-printed with their appropriate UPC bar code. The expiration date information (i.e., good until xx/xx/xx) is stamped onto the label after the container is filled.

Because expiration date information is meant to be visually apparent to an ultimate consumer, such information is not expressed in electronic form (i.e., in bar code or RFID form). There is no efficient method by which expiration periods can be electronically acquired from an item's packaging and stored for processing and expiration date management by an ultimate consumer. Consumers must manually record freshness periods and engage in complex and time consuming inventory control activities in order to manage their food inventory. The problem becomes even more complex once it is realized that large classes of perishable goods, i.e., fresh fruits and vegetables, are not identified with any form of expiration date information.

Thus, there is a need for a system and method for acquiring expiration date and/or "freshness" information with respect to all classes of perishable goods and for simply and efficiently transferring this information to a consumer so that the consumer may maintain a perishable inventory control system with a minimum of effort, preferably without requiring any human intervention. The system and method should reflect not only an item's expiration date, but also the "freshness period remaining" after the package is open, as well as provide an alert when an item is approaching its expiration date.

SUMMARY OF THE INVENTION

These and other objects are accomplished in accordance with the present invention by providing the purchaser with electronic inventory control systems and methods for managing limited-shelf-life products.

More specifically, the present invention provides apparatus, systems and methods by which information concerning the shelf-life limitations of a particular product item is made available to the purchaser electronically; that the electronically recorded shelf-life limitation information is provided to, or made accessible by, the purchaser; that the electronically recorded shelf-life limitation information is communicated to a computer equipped with a microprocessor, or to a computer system network, accessible by the purchaser, programmed to receive the shelf-life limitation data for each product for that purchaser; that the computer or purchaser-accessible computer system network, is further programmed to provide the purchaser with on-screen and/or printed reports of various formats that list the items purchased and the corresponding shelf-life limitation information; and that the computer or purchaser-accessible computer system network provides interactivity with the purchaser to allow the purchaser to identify further information to the computer/network, such as identifying location information of each particular product item, and the inventory status of each particular product item, e.g., whether the product has been opened or has been discarded.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features, aspects and advantages of the present invention will be more fully understood when considered with respect to the following detailed description, appended claims and accompanying drawings wherein:

FIG. 1 is a simplified, semi-schematic diagram of an expiration date management system in accordance with the present invention, utilizing bar code information;

FIG. 2 is a simplified, semi-schematic diagram of an expiration date management system according to the present invention utilizing RFID labeling;

FIG. 3 is a simplified, semi-schematic block diagram of an exemplary expiration date database including item description information, an item identification code (UPC code) and expiration date information;

FIG. 4 is a simplified, semi-schematic layout diagram detailing an exemplary organization of an electronic receipt;

FIG. 5 is a simplified, semi-schematic block diagram of the system configuration of an exemplary home terminal;

FIG. 6 is a simplified, semi-schematic layout diagram detailing the organization of an exemplary expiration date listing; and

FIG. 7 is a simplified, semi-schematic diagram of a touch panel screen display of a home terminal, detailing the organization of a purchaser's exemplary expiration date listing.

DETAILED DESCRIPTION OF THE INVENTION

In accordance with the present invention, expiration dating information pertaining to large classes of perishable goods, such as grocery items, is acquired for each of the items stocked by a particular store and maintained in such a manner as to make this information available to a consumer in the form of an electronic receipt. Once the information on an electronic receipt has been transferred to the consumer, this information is used to generate and maintain a residential inventory control system on a home terminal, for example. Thus, shelf life limitations of particular perishable items are provided to a consumer in a form transported to and processed by home electronic equipment.

There are several different types of shelf life limitation information that are associated with certain individual perishable products. Particularly, such information pertains to the shelf life of the item, i.e., the expiration date for the unopened product, and the freshness period for which the product remains viable once it has been opened. In accordance with the present invention, shelf life limitations (expiration date information) for any particular product item is acquired and recorded in such a way that it is made electronically available to the purchaser of the item, such that the expiration date information is directly associated with a particular product item.

FIG. 1 depicts a simplified, semi-schematic diagram of an exemplary expiration date management system in accordance with the present invention, in which expiration date information is acquired, transferred and processed for any particular perishable item, in connection with a corresponding bar code item identifier. As depicted in FIG. 1, a consumer selects items to be purchased, in conventional fashion, and loads the items into a utility shopping basket. Once the consumer completes the shopping trip, the consumer takes the shopping basket to a checkout station where items are identified at a point-of-sale terminal **10** by scanning the selected items with a bar code scanner **12**. In conventional fashion, the bar code scanner **12** picks up an item's UPC (Universal Product Code) or SKU (stock keeping unit) code from a bar code printed on each item's product label when the label is manufactured, or printed and attached locally in the store.

Suitable bar code information is electronically processed by the point-of-sale terminal **10** in order to identify the item description (item name) and item price. In addition, and in accordance with the practice of the present invention, the bar code information scanned from each particular item is transmitted to a store platform computer **14** which might be configured as a network server, or some other form of platform data processing unit. Once an item has been identified to the store server **14**, the server system consults a database **16** which contains all of the requisite information pertaining to any item of merchandise sold by the store, including expiration date information, associated to individual merchandise items through that item's PLU or SKU code read by the bar code scanner **12**.

In a manner to be described in greater detail below, the server system fetches the requisite information relating to each item scanned for purchase, and redirects that information to the POS terminal **10** where it is appended to an electronic transaction log file, termed herein an electronic receipt **18**. It should be noted that the electronic receipt **18** is generated in addition to a conventional paper receipt of the form normally provided to a customer at time of check out. The electronic receipt **18** might be the primary and only receipt generated with regard to that particular transaction, i.e., the paper receipt might be provided optionally or not at all, at the option of a retail facility. Since the electronic receipt **18** is in electronic file form, the receipt might be given to the customer directly as the customer completes his transaction of the POS terminal **10**, or alternatively, the electronic receipt **18** might be electronically transferred to a web server **20** belonging to the retail facility, where it is maintained in an electronic file storage area **22** for eventual retrieval by the consumer.

A direct transfer of the electronic receipt **18** to a consumer might be accomplished by issuing the consumer with a purpose-designed IC card which would necessarily include sufficient memory storage space into which an electronic receipt might be written. Various forms of IC cards are contemplated for use with the present invention. Examples of such IC cards include a common rigid plastic card that incorporates a high-density magnetic stripe, suitable for reading and writing electronic information, a wireless RF-type card which includes a semiconductor memory, or a contact-type IC card. All of these forms of IC cards are well understood by those having skill in the art and the appropriate types of equipment required to read from and write to such IC cards are readily available and, indeed, in common use in various types of retail facilities. Writing an electronic receipt to a customer's IC card offers the customer a simple and efficient method of receiving an electronic receipt from a grocery store, for example, and for transporting the electronic receipt to a remote location, such as the home, for read out, evaluation and further processing.

Hosting the electronic receipt in a file or memory storage area **22** of a retail facility's web server **20** allows the customer the freedom of being able to shop in multiple stores without the necessity of carrying multiple types of IC card, one card for each different store. As electronic receipts are loaded into the file or memory storage area **22** of each store's web server **20**, the electronic receipts are available for a customer to access and download, once the customer reaches home and accesses each store's server **20** through the customer's Internet connection **20**. By signing on to the Internet, and visiting each store's web site in sequence, the customer is able to download each electronic receipt maintained by each of the stores that customer has visited during the latest shopping trip.

In the home environment, electronic receipt retrieval and processing for expiration date management is preferably performed by a purpose built electronic home terminal unit **24** which is located in proximity to a refrigerator, if the items being expiration date managed are grocery items, for example. Although located in proximity to a refrigerator **26** or even mounted on the refrigerator unit or in a door thereof, the home terminal **24** includes appropriate communication interface hardware and software to enable it to receive electronic receipt information, either from a consumer, by reading the information contained on the consumer's IC card, or by contacting a store's web server **20** and accessing the file or memory storage area **22** for the appropriate electronic receipt. Such appropriate communication interface hardware and software might include a modem configured for Internet communication through a telephone subscriber line interface, an ISDN interface, cable modem and cable connection, an IC card reader/writer unit, their appropriate controlling application software, and the like.

In addition, the home terminal **24** also includes some means of scanning, or otherwise identifying, items that have been recently purchased and are to be stored in the refrigerator unit **26** with which the home terminal **24** is associated. If item identification is made at the retail store with a bar code, the home terminal **24** will suitably include a bar code scanner **28** with which the bar codes of purchased items may be scanned and entered into the terminal's memory for further processing. As will be described in greater detail below, the identification means need not be a bar code scanner. Various retail facilities often identify their goods with an RFID tag either alone, or in combination with a bar code. If item information is obtained from reading an RFID tag by the store, the home terminal **24** will likewise be provided with an RFID receiver unit so that an accurate and timely inventory might be taken and maintained of items identified by RFID tags.

Such a system, in accordance with practice of the present invention, which utilizes RFID tags for merchandise identification, is illustrated in the simplified, semi-schematic system diagram of FIG. **2**. Since the system, in accordance with the invention, depicted in FIG. **2** is generally similar to the system illustrated in FIG. 1, and contains a number of common elements, those common elements will be identified with the same numeral as the corresponding element of FIG. **1**. Thus, items to be purchased will be taken to a POS terminal **10** comprising a checkout station. The POS terminal **10** need not be a conventional checkout station such as one operated by a store clerk, but might also be a self operated checkout terminal, a kiosk-type checkout terminal, a portable customer operated self-scanning terminal, and the like. No matter what form taken by the POS terminal **10**, the terminal system necessarily includes an RFID reader unit **30** which is configured to interrogate RFID labels **31** disposed on individual items of merchandise and retrieve the item information contained in each RFID label. An RFID capable terminal is able to read all of the RFID labels of all purchased items in a shopping cart or shopping basket in a single operation, without the need for human intervention. RFID labels conventionally contain at least some form of identification code (a PLU code, UPC code or SKU code) specific to the particular item to which the RFID label is attached. The checkout station terminal **10** identifies all the purchased items by the corresponding item code (PLU, SKU or UPC), and accesses an item information database (PLU table, for example) **16** hosted by a store server **14**, in order to obtain item information such as the item name, item price, associated discounts, and the like, for each purchased item.

In addition, the checkout terminal **10** is able to retrieve expiration date information and freshness period information for each tagged item, by accessing the appropriate item database files or PLU table fields of the information database **16** for each item. Once all of the requisite information is obtained for each item identified by an RFID tag, the checkout terminal **10** generates an electronic receipt **18**, the form of which will be described in greater detail below.

As was the case with the exemplary embodiment of FIG. **1**, the electronic receipt **18** is either provided directly to the customer, by writing the electronic receipt information into a memory storage area of an IC card or alternatively, the electronic receipt is transmitted to the store's web server **20** where it is stored in a local file or memory storage area **22** for eventual retrieval. It should be noted, that in both the exemplary embodiments of FIGS. 1 and **2**, that the electronic receipt need not necessarily be generated by the POS checkout terminal **10**, before transmission to the store's web server **20**. Indeed, all of the requisite information acquired with regard to each individual item tô be purchased might be processed by the facility's store server **14** in order to generate an electronic receipt. In addition, if the system were configured to make electronic receipts available to consumers only through a web server-type arrangement, it will be understood that the web server is equally capable of processing each item's associated information in order to generate an electronic receipt. Thus, the electronic receipt is able to be generated by any of the electronic data processing equipments contemplated by the system of the present invention.

Returning to FIG. 2, once generated, the electronic receipt **18** is made available to, and processed by, a home terminal unit **24** disposed in proximity to the place where perishable, expiration dated goods are to be stored, such as a home refrigerator **26**. As was the case with the illustrated embodiment of FIG. **1**, the home terminal **24** is configured to include communication interface hardware and software which will allow the home terminal to access an electronic receipt storage means and retrieve the electronic receipt **18**. If the electronic receipt is provided directly to a customer by means of an IC card, the home terminal **24** will necessarily include an IC card reader/writer unit, configured to interface with a customer's IC card. The home terminal is additionally configured to include an RFID reader **29** to enable the terminal to read RFID tagged goods, as will be described further below. The RFID reader **29** is suitably disposed such that it is able to interrogate RFID labeled goods inside the refrigerator **26** and automatically identify whether items have been added or removed from the refrigerator contents. Likewise, the home terminal **24** is configured with communication interface hardware and software such as a telephone line modem, cable modem or any other communication interface which allows communication between the home terminal **24** and the web server **20** hosting the electronic receipt.

Pertinent to the configuration of the home terminal **24**, is the realization that its function may be performed by a number of different systems. For example, the functions of the home terminal are easily performed by a conventional personal computer (PC) which might even be configured as a lap top. In addition, the home terminal might suitably be implemented as a reduced function PC, such as a web terminal (a purpose-built processor containing Internet access hardware and software and including a web browser). The home terminal function might also be accomplished by an Internet TV, a web TV or other, similar devices having communication interface circuitry, Internet access and some degree of processing power. The home terminal, when used for expiration date management of grocery items, could be configured so as to be easily mounted on the door of a refrigerator. The terminal includes at least a display and some means for inputting data, such as a touch sensitive screen, a keyboard, a keypad and/or speech recognition processing. Depending on the system configúration, the terminal optionally includes an RFID reader interface, bar code scanner interface and/or a Smart Card reader/writer interface. In the case where the system is configured to operate in conjunction with products that are identified by RFID tags, the RFID reader unit **29** is preferably installed inside the refrigerator in order to be in sufficient proximity to the items to identify RFID labeled items stored therein.

As was described above, in connection with the exemplary embodiments of FIGS. **1** and **2**, expiration date information and freshness period information for any particular perishable item stocked by a store can be associated with that item in a number of ways. As a particular item is manufactured or packaged, that item's expiration date and/ or freshness period information is associated to that item by the manufacturer. Typically, this is done by stamping or otherwise affixing an expiration date onto the product package and/or including a freshness period warning among label contents, i.e., use within three days after opening.

In one embodiment of the invention, as a store, such as a grocery store, receives merchandise from a wholesaler or distributer, the expiration date and freshness period information associated with each item of merchandise received in a shipment is entered into the store's merchandise inventory database system along with each item's UPC or SKU code information. When such information is entered into a store's database, it is often compiled in what is termed a PLU (Price Look Up or Product Look Up) table. PLU tables are typically organized by an individual item's UPC or SKU number and include fields associated with an item's code that identify the name of the item, the item price, and the like. A store's inventory management system might be implemented as an expanded form of PLU table with a number of items in inventory field appended to the typical item identification fields. As new items are received in inventory, each item's bar code or RFID label is scanned or read and the inventory field associated with that particular code is incremented. According to the invention, expiration date and freshness period information are also entered into the system's database as new items of merchandise are added to system inventory. Since bar code and RFID labels include lot number and time stamp information, it is a relatively simple matter to keep track of expiration date information with respect to different shipments of similar goods that arrive at different times. In one embodiment of the invention, expiration date and freshness period information is contained in an appropriate field or fields which are appended to the item information fields contained in a PLU table.

A further embodiment of the invention contemplates maintaining expiration date and freshness period information in an "expiration date database". Such a database is similar to a PLU table, but is constructed of a truncated set of information fields. As depicted in FIG. 3, an expiration date database is constructed of a set of entries, with each entry identifying a particular perishable item by its corresponding UPC code (or SKU number). An expiration date is associated to each UPC code, as is a freshness period after the package is open. If the expiration date database is constructed to include only perishable items, it is axiomatic that each item will have an associated expiration date. However, not all items will have a varying freshness period depending on whether or not the item has been removed from the package. For example, fresh fruits and vegetables will be understood to have an expiration date, i.e., a period after which they become rotten, but do not necessarily have a variable freshness period. In contrast, many items, such as canned fruits and vegetables, will have an expiration date extending far into the future, but have a relatively short freshness period, i.e., 7 to 10 days, after the can has been opened. The expiration date database makes all of this information available upon entry of the appropriate corresponding UPC code.

Thus, as a particular item is being purchased by a customer and that item's code is either scanned by a bar code scanner or accessed by an RFID reader, that item's expiration date and freshness period information is extracted from the database either from that item's PLU table entry or from information entered into an expiration date database.

As an alternative to database or PLU table entry, an item's expiration date and/or freshness period information may be embedded or appended to machine readable item identification means (bar code or RFID tag) affixed to an item's packaging. Expiration date information and/or freshness period information might be provided as part of an extended bar code or as a second bar code printed on the product packaging as the item is ready to ship. Likewise, expiration date information and freshness period information might be appended to the conventional information provided in an RFID tag. Thus, rather than defining a link to the expiration date and freshness period information contained in the database, an item's bar code and/or RFID tag contains all of the requisite information associated to that item.

As an item is scanned by a bar code scanner or interrogated by an RFID reader, the bar code or RFID information is electronically read and interpreted in order to retrieve that item's expiration date and freshness period information.

It should be understood that the particular illustrated embodiments of the invention depicted and described in connection with FIGS. 1, 2, and 3, are not intended to be limiting as to how expiration date and freshness period information is acquired or stored. It should be understood that an item information database may be implemented as a PLU table, a subset of a PLU table, as a relational database, and the like. Further, the database need not be hosted on a platform server, but it might be stored locally at each checkout station or POS terminal. The database need not even be locally available, but rather it might be accessible through an Internet connection from an enterprise-wide platform system or even constructed "on-the-fly" by accessing different web sites for each particular manufacturer as indicated by the item's bar code or RFID label.

Further, the expiration date and freshness period information need not necessarily be provided as an adjunct to conventionally understood bar codes or RFID labels. An additional method to make expiration date information available in a machine readable form is to print the expiration date and freshness period information on the product label in a machine-readable font, such as is used to identify codes on airplane tickets. The alpha numeric information is scanned by a receiving retailer when the product is entered into inventory and the information is interpreted by an application software program into recognizable expiration date an/or shelf life limitation information in an electronically storable form.

In accordance with the present invention, expiration date and freshness period information is provided to, or made accessible to, the purchaser along with other pertinent information about each item purchased, in the form of an electronic receipt. Once all of a customer's items have been bar code scanned or RFID interrogated, and the purchaser has paid for the items, an electronic receipt is generated, often in conjunction with an optional conventional paper receipt.

FIG. 4 depicts the layout organization of an exemplary electronic receipt, in simplified, semi-schematic form. As shown in FIG. 4, a typical electronic receipt will include certain demographic information such as the customer's name, a unique identification tag issued by the store in order to identify that customer (a customer ID), the name of the store issuing the receipt, and the time and date of the shopping excursion. Additionally, an electronic receipt includes the same types of information associated with conventional paper receipts, such as the name of each item or its description, the quantity of each item purchased and the price paid for the item. The electronic receipt also includes entries for the total price paid, sales tax information, and the like.

In accordance with the invention, the electronic receipt further includes certain information not normally contained in a conventional paper receipt. This information suitably comprises each item's UPC code, with each code entry associated with its corresponding item, an expiration date entry and a freshness period entry, each associated to its corresponding item through that item's UPC code. Thus, as indicated in FIG. 4, the customer purchased two portions of low fat cream cheese at a price of $5.96. Low fat cream cheese has a UPC code of 41334444 and an expiration date of Sep. 30, 1999. The low fat cream cheese item purchased by the customer has a residual freshness period of 10 days after the package has been opened, after which the item is no longer safe for consumption. Further, as is indicated in FIG. 4, items such as Fuji apples and low fat milk have an expiration date but no residual freshness period. Likewise, items such as tissues and shampoo have neither a residual freshness period nor an expiration date. All of the information contained in the exemplary electronic receipt of FIG. 4 is able to be retrieved electronically by whatever form of system is preparing the electronic receipt. Typically the item description and item price information are acquired from the store's PLU table, as is the UPC information. Expiration date and freshness period information is acquired either from the store's PLU table, an expiration date database, or from an extended bar code or an extended RFID label affixed to the product.

As was described above, the electronic receipt can either be recorded on a Smart Card or IC card and presented to the purchaser upon checkout or alternatively, the electronic receipt can be delivered through a communications network, such as the Internet, typically through a store server, to a particular web server. The web server stores the purchasers electronic receipt in a database of electronic receipts where it may be suitably accessed by either the consumer or by a home terminal, such as will be described further below. In an embodiment where the electronic receipt is saved in a database of receipts, it will be understood that appropriate password protection will be given to the electronic receipt information such that only the appropriate purchaser can access the information. For example, the customer might identify themselves with their customer ID, which is matched to the customer ID field comprising a receipt.

In accordance with the present invention, the expiration date and/or freshness period information, included in the electronic receipt along with the item description and the item's UPC code, is communicated to a computer equipped with a microprocessor, or to a computer system network, accessible by the purchaser, and programmed to receive the information contained in an electronic receipt for each product item purchased by that purchaser. In a residential embodiment, the computer system might be implemented as a home PC, a web terminal, Internet TV, web TV a specialized purpose-built "kitchen terminal" or the like (all referred to herein with the common term "home terminal"). FIG. 5 is a simplified, semi-schematic block diagram of an exemplary system configuration of a home terminal, suitable for practice of the present invention. As seen in FIG. 5, one embodiment of a home terminal includes a display screen 60 which might be implemented as a "touch screen" or touch panel display. The display screen 60 is coupled to and controlled by a central control unit 62 which performs the primary processing functions of the home terminal and which includes a microprocessor, a signal processor, or some other such form of central processing unit.

The purchaser is able to transfer the contents of the electronic receipt to the home terminal in any one of a number of ways. The home terminal has the provision for being connected to an optional Smart Card reader/writer 64 with which to access the electronic receipt information recorded on a Smart Card or IC card by the store where the purchaser bought the product items. Alternatively, a communication interface 66, such as a modem, cable modem or other similar communication interface device, enables a home terminal to contact an off-site location, such as a store web site, where it is able to access and download an electronic receipt. It should be noted that in the case where the electronic receipt is stored on a web server, the web server is able to automatically generate an e-mail to the purchaser's home terminal in order to notify the purchaser that the electronic receipt is available for access or download. Pertinent to the communication interface 66 is that the interface is coupled to a global communications network, such as the Internet, via a communication link such as a telephone subscriber line, ISDN line, cable, satellite, or other similar form of communication link. However accessed, whether through the Smart Card reader 64 or the communication interface 66, the electronic receipt information received by the home terminal is stored in a local memory storage area 68 which might be implemented as Read Only Memory (ROM), Random Access Memory (RAM), a hard disk drive, or the like.

In order to account for changes in a purchaser's perishable goods inventory, the home terminal is suitably provided with various means to identify products as they are introduced to a refrigerator, for example, by the purchaser. In this regard, the home terminal includes a bar code scanner 70 coupled to a bar code scanner interface 72, in turn connected to and controlled by the home terminal's control unit 62. The bar code scanner 70 functions to identify the introduction of goods that are identified by bar codes that have been pre-printed on the product label, for example. In addition, in cases where certain merchandise items are identified and tagged by RFID labels, the home terminal is suitably provided with an RFID reader 72, coupled to and controlled by the control unit 62 which is able to interrogate and identify a product's RFID label through an integral antenna 74.

Thus, it should be understood that the home terminal has generally the same capabilities of recognizing a product, particularly with respect to the product's UPC code, as the store from which that product was purchased. In the case of the store, the product indicia (the bar code or RFID label) was translated to a UPC number (in its simplest form) which was then used to access a store database in order to acquire additional information about that product. In the case of the home terminal, generally the same apparatus (bar code scanner or RFID reader) is used to acquire the same product indicia which, in a manner to be described in greater detail below, is used to identify recently purchased perishable goods and to invoke the terminal's expiration date management system.

In operation, the home terminal (24 of FIGS. 1 and 2) is used to specify items that have been purchased and that will be stored in a refrigerator, for example, by the purchaser (i.e., used to inventory items). Specifying newly purchased items depends on whether the items are identified by a bar code label or by an RFID label. In the first case, items are specified to the home terminal by depressing an "IN" key or button, indicating that the terminal is to download an electronic receipt and add the newly purchased items into terminal memory. In the case of items identified by an RFID label, the home terminal's RFID reader 72 identifies the addition of newly purchased items by periodically interrogating the contents of the refrigerator and, if new items are discovered, the terminal downloads the appropriate electronic receipt. After items have been identified to the terminal as newly purchased, the control unit, under appropriate software program control, obtains the corresponding electronic receipt from the store's web server either by Internet mail or direct web site access. In this particular circumstance, the customer name, customer ID, store name and shopping date and time are used as key associative information for electronic receipt retrieval. If the electronic receipt is provided to the purchaser by means of a Smart Card or IC card, the home terminal control unit would display a "insert Smart Card" message to the consumer and subsequently read the contents of the Smart Cart or IC card in order to obtain the electronic receipt information.

Once the electronic receipt is obtained, by either access means, the items listed in the electronic receipt are added or appended to an internally maintained file comprising a list of stock items (i.e., an inventory list). Depending on the particular configuration desired, either all of the items included in the electronic receipt are added to the list of stock items or, alternatively, only items which have expiration date information are captured and are added to a list of expiration date stock items.

FIG. 6 is a simplified, semi-schematic illustration of an exemplary "expiration date list" such as might be obtained and constructed from the electronic receipt information depicted in FIG. 4. The exemplary expiration date list of FIG. 6 is constructed to include an item description field for each item captured from the electronic receipt, an item quantity field, a purchase date field and particular fields denoting expiration date and freshness period information captured from an electronic receipt.

Turning now to FIG. 7, which is an exemplary home terminal screen display of the expiration date list of FIG. 6, the operation of the home terminal will now be described in connection with a particular set of control functions, illustrated as function buttons in the exemplary embodiment of FIG. 7, when the display screen is implemented as a touch screen panel. Briefly, the touch panel is used to specify the various control functions as well as providing an alpha numeric character input for manual item data input. When configuring the screen as an alpha numeric input, a special function button such as "home" **76** or "help" **78** might be selected to invoke a function menu from which a keypad configuration might be selected for manual data input. However, the operation of the home terminal in accord with the present invention will be described in connection with automatic item data entry for ease of explanation.

In order for the terminal to develop and maintain a stock record of items stored in a refrigerator, it is necessary to indicate to the terminal that newly purchased items have been added to the current stock. Since items identified by bar code labels cannot be automatically identified to the terminal, these items are identified to the home terminal unit as added items, by the user, by depressing the "IN" key **80** on the touch screen panel of the home terminal display screen **60**. When the "IN" key **80** is depressed, an application software program resident in the home terminal understands that additional items are to be added to the list maintained in memory and issues the appropriate commands to launch a web access routine and request the latest electronic receipt information from a web server, for example, using the customer's name, customer ID, store name and shopping date and time, as key index fields for receipt retrieval.

Alternatively, if an electronic receipt is provided by a smart card, the control unit (**62** of FIG. **5**) causes the screen to display the message "insert smart card". Once the smart card is inserted into the smart card reader (**64** of FIG. **5**) the terminal reads the contents of the card to obtain the electronic receipt information.

Once the electronic receipt information is received (either from the web server or from a purchaser's IC card) the home terminal system may either append all newly purchased items to the current stock list or, alternatively may only append those items which contain expiration date information to the current list. Where the terminal is configured to append all newly purchased items to its current stock, the user is able to manually edit the list by selecting certain items which do not have expiration dates, i.e., tissues, and depressing the OUT key or button **84** on the terminal's touch panel screen. Thus, the home terminal system is able to create and maintain a current stock list (expiration date list) comprising an item name or description, a quantity field, a purchase date field, and fields related to each item's expiration date and/or corresponding freshness period.

Items labeled with RFID tags are able to be automatically sensed by the terminal and newly purchased items can be automatically identified. The terminal periodically interrogates the refrigerator contents, by asserting an RF interrogation signal, to determine if any newly purchased items have been added. Each item in the refrigerator provided with an RFID label responds with its label contents, i.e., its UPC code. The control unit compares the current inventory with the previous inventory and, if any newly purchased items are present, invokes an application program. As described previously, the program retrieves an electronic receipt, either from a store web page or by requesting the customer to insert a smart card containing electronic receipt information. Once the electronic receipt is obtained, expiration date information and other related indicia is matched to the newly added items by the UPC code.

Since it is sometimes the case that a certain number of purchased items are not labeled, either with a bar code or with an RFID label, it becomes necessary to manually inform the home terminal unit that certain items are being added into perishable item inventory. This is also the case where a particular store does not have the capability of creating an electronic receipt.

In either case, items may be manually identified to the home terminal unit by depressing the IN key or button **80** on the touch panel screen. When IN is depressed, and no electronic receipt is available, the corresponding I/O devices such as the bar code scanner (**70** of FIG. **5**) or RFID reader (**72** of FIG. **5**) are activated for manual entry. Manual data entry can be done by scanning an item's bar code, reading the contents of an RFID label or by reconfiguring the screen for alpha-numeric keyboard entry. Thus, the present invention is able to accommodate manual data entry when necessary, even though it is primarily configured to minimize human intervention.

Once the list is created, a purchaser is able to review the contents of the list by depressing a "LIST" key **82**. As shown in the exemplary screen display of FIG. **7**, the inventory list includes not only a list of expiration dated products, but also a sub-list of "near expired items" as well as an additional sub-list of "already expired items". The "near expired items" list is a purpose defined subset of the complete expiration date list but includes those selected items whose expiration date is calculated as being within a pre-defined time period of the current date and time (i.e., today). As depicted in FIG. **7**, two packages of spinach have an expiration date of Jan. 3, 1999, which is only one day away from the current date of Jan. 2, 1999. Likewise, a package of mushrooms has an expiration date of Jan. 4, 1999, only two days away from the current date.

The "already expired items" list includes those items whose expiration date has already passed. Likewise, the "already expired items" list might also include those items whose expiration date has not yet been exceeded, but which have been opened for a period longer than their stated freshness period.

In this regard, the user is able to identify when a particular perishable item's package has been opened by depressing the OPEN key 83 of the touch screen panel of the home terminal. Once the OPEN key has been depressed, the user selects which of the items have indeed been opened by scrolling through the perishable item list and selecting the specific item whose container has just been opened. The user might, for example, select the OPEN key 83 and then choose low·fat cream cheese as the item which has been opened. Since there are two quantities of low fat cream cheese indicated in the list, only one will be selected unless the user chooses to select the second. For the item selected as being open, the system begins a countdown clock which decrements the freshness period entry by 1 for each passing calendar day. Thus, the low fat cream cheese entries for Jan. 4, 1999 would include 1 entry having a freshness period of 10 days and a second entry having a freshness period of 8 days.

Once an item has been exhausted, or the user desires to remove an item from storage either for consumption or because it has exceeded its expiration date period, the user selects the OUT key 84 which indicates to the home terminal system that an item or items will be deleted from the list. After the OUT key 84 has been selected, the user again scrolls through the list of items in order to select the item or items which will be deleted. If, for example, the user consumes all of one quantity of low fat cream cheese, the perishable item inventory list will only have an entry for 1 quantity of low fat cream cheese remaining.

It should be understood that in the case of goods identified by an RFID label, the user need not concern themselves with use of the IN 80 or OUT 84 keys in order to indicate to the home terminal that items have been added or deleted from inventory. Where the system contemplates the use of RFID labels, the system is configured to automatically and periodically interrogate the contents of the refrigerator and compare the return values with the perishable item inventory list. In this manner, both newly added items and newly deleted items will be immediately identified by comparing the results of the present interrogation with the next prior one's results. It should also be noted that if the item is identified by a bar code, the user is able to identify that item's deletion by depressing the OUT key 84 and then by scanning the item's bar code. This informs the system that that item has been deleted and its entry is consequently removed from the perishable item inventory list.

Notwithstanding the foregoing, it should be understood that the operation of the home terminal unit has been described in connection with the above-exemplary embodiment for the case where an item bar code or an item RFID label contains only the item identification code (i.e., a UPC code or an SKU code). In the case where additional information is included as an extended bar code or an additional bar code pre-printed on a package label or additional information is included in the contents of an RFID label, there may be no need for the home terminal unit to consult an electronic receipt in order to generate a perishable item inventory list with all of the necessary data fields included therein. Depending on the type and amount of information included in either a bar code or an RFID label, it will be understood by those having skill in the art that the home terminal unit may need to consult an electronic receipt for a reduced subset of information contained thereon. For example, if the bar code or RFID label contains an expanded set of product identification information, the home terminal unit may only need to consult an electronic receipt in order to obtain expiration date and/or freshness period information. The home terminal will thus be understood to be a rather flexible device with regard to how information is obtained in order to construct the perishable item inventory list. Data input can be anywhere from completely manual to completely automatic (not requiring any human intervention) depending on the type and manner of item coding (i.e., bar code or RFID label) and the type and manner of system interrogation and data processing.

Thus, according to the invention, the system has present utility when an electronic receipt is used in conjunction with a conventional product code such as a bar code or an RFID label. The product code functions as a key which points to product name, description, price and expiration date information in the retail store environment. Likewise, the product code is used as a key in defining which items are to be added to perishable item inventory in the home environment. In the home, a home terminal uses the key to select items from an electronic receipt for addition to a perishable item inventory list. The perishable item inventory list includes the same type of product name, description, expiration date and/or freshness period information which was matched to a corresponding item in the retail store through the product code key. Use of an electronic receipt does not require changing current bar code application procedures nor does it require printing of additional information on product packaging when perishable contents are introduced to a package or container.

In future use, particularly in the case of an RFID label with expanded capabilities, all information may be easily incorporated into an RFID label and such information may be automatically captured by a home terminal unit upon that product's introduction into perishable item inventory storage. Thus, both electronic receipts and human intervention are no longer required for the addition or deletion of perishable items from a perishable item inventory list. While the invention has been described in connection with particular illustrated embodiments, those skilled in the art and technology to which the invention pertains will have no difficulty devising variations which in no way depart from the scope and spirit of the present invention. For example, while the illustrated embodiments have been described in connection with consumer shopping and home usage, it will be appreciated that the present invention may be adapted for utilization in restaurants, pharmacies, hospitals, and the like. Further, it will be understood that although the term "purchaser" has been used throughout the above-specified description, the term "purchaser" includes the individual that actually purchases the product items and anyone else able to operate the system in the case of home use of the invention. Accordingly, the present invention is not limited to the specific embodiments described above, but rather is defined by the scope and spirit of the appended claims.

What is claimed is:

1. A method for managing product items with shelf-life limitations comprising the steps of:

associating shelf-life limitation information to each of one or more perishable product items;

recording said shelf-life limitation information for each of said one or more perishable product items in a database;

identifying selected ones of perishable product items being purchased;

recovering said recorded shelf-life limitation information from the database for each of the perishable product items selected for purchase;

electronically recording said shelf-life limitation information for each of said one or more product items in an electronically readable and storable form;

providing the shelf-life limitation information to a purchasing customer in the electronically readable and storable form; and

using a terminal accessed by the purchasing customer to add the shelf-life limitation information to an inventory list, the inventory list being used by the purchasing customer to manage use of the said one or more product items.

2. The method according to claim 1, further comprising the step of transferring said electronically recorded shelf-life limitation information to a memory storage area.

3. The method according to claim 2, wherein the shelf-life limitation information is recorded on an electronic receipt, the electronic receipt being transferred to a memory storage area of a web server.

4. The method according to claim 2, wherein the shelf-life limitation information is recorded on an electronic receipt, the electronic receipt being transferred to a memory storage area of a smart card.

5. The method according to claim 2, further comprising the steps of:

retrieving the shelf-life limitation information from the memory storage area; and

displaying the electronic shelf-life limitation information for each of said one or more product items on a home terminal display screen.

6. The method according to claim 5, wherein the recorded shelf-life limitation information is electronically recovered from the database by a store check-out terminal.

7. The method according to claim 6, wherein the store check-out terminal electronically recovers the recorded shelf-life limitation information for each perishable product item by scanning a bar code each item and associating each item's bar code with an entry in the database.

8. The method according to claim 6, wherein the store check-out terminal electronically recovers the recorded shelf-life limitation information for each perishable product item by reading an RFID label affixed to each item and associating each item's RFID label information with an entry in the database.

9. The method according to claim 6, wherein the database comprises a price-look-up table, shelf-life limitation information for each perishable product item being associated to that item according to its corresponding entry in the price-look-up table.

10. The method of claim 1, wherein the shelf-life limitation information includes a period for which the product remains viable once it has been opened.

* * * * *